

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-225143

(43)Date of publication of application : 17.08.1999

(51)Int.Cl.

H04L 9/32
G06F 17/60
G06K 17/00
G07B 1/00
G07B 5/00
G07F 7/12
G09C 1/00

(21)Application number : 10-027074

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 09.02.1998

(72)Inventor : KIKO KENICHIROU

NAKAGAKI JUHEI

KIYOUJIMA HITOKI

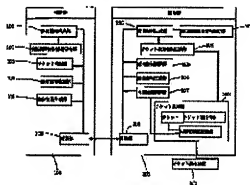
TANIGUCHI SHINICHIRO

(54) ELECTRONIC TICKET SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an internal state of a certificate device from being revised due to a ticket exhibited by mistake or illegally.

SOLUTION: An authentication information generating section 102 of an authentication device 100 generates authentication information and sends it to a certificate device 200. A ticket discrimination information generating section 203 of the certificate device 200 generates ticket discrimination information to indicate storage of a correct ticket from ticket utilization information and information in an internal state storage area. A certificate information generating section 206 connects ticket discrimination information to low-order bits of a bit stream of the authentication information to generate ticket certificate information. The ticket certificate information is sent to the authentication device 100 by a communication section 208. The authentication device 100 receiving the ticket certificate information conducts ticket discrimination processing and



terminates the protocol when the ticket certificate information is incorrect or the ticket is not to be authenticated.

LEGAL STATUS

[Date of request for examination] 20.09.2002

[Date of sending the examiner's decision of rejection] 23.08.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the technique of creating a ticket and a card electronically and using them.

[0002]

[Background of the Invention] The attempt which publishes common tickets, such as a ticket, an admission ticket, a reserved seat ticket, a reservation ticket, a coupon ticket, a commuter pass, a prepaid card, and a point card, as an electronic ticket is performed in recent years [[conventional technical]].

[0003] A publisher can specify the right granted to the user and such an electronic ticket has the function in which it is verifiable that it is a right ticket. Electronic intelligence is easy to create, and although it has the features that it can transmit through a communication line, since a perfect copy can be made easily, the cure to the unjust use by forgery and the duplicate is indispensable to implementation of an electronic ticket. Although prevention of forgery by electronic signature is possible, prevention of a duplicate is difficult, and preventing the unjust use by the duplicate had become the biggest technical problem were in charge of implementation of an electronic ticket.

[0004] The three approaches of of the user just to the utilization time of the former and a ticket as a solution, the 1st conventional technique to check, the 2nd conventional technique which does not give an opportunity to copy a ticket at persons other than a publisher, and the 3rd conventional technique which corrected the 2nd conventional technique so that the communication link at the time of verification could be exhibited over this problem have been proposed.

[0005] The 1st conventional technique is the approach a user checks whether you are a just user to the utilization time of a ticket, and a user shows with a ticket that he is the just user to whom he suits user specific information, when using a ticket. If it conforms to user specific information, use of a corresponding right will be accepted. Information which matches information (user specific information) required for a check and the granted right is published as a ticket, and a user keeps records. In order for persons other than a publisher to prevent from forging a ticket freely, a publisher performs electronic signature to a ticket. The ticket without electronic signature is judged to be what was forged. Possession of the knowledge of the bodily features of an identity, a photograph of his face, etc., a password, etc. can be used for user specific information.

[0006] However, by this approach, some troubles arise according to the user specific information to be used.

[0007] For example, by the approach of using a user's identity for user specific information, a user will be identified at the time of issue and verification, and anonymity will be lost. Moreover, since the method of proving a status safely in the remote environment using a communication line is not realized, in such an environment, a thing without a just right cannot prevent using a ticket unfairly.

[0008] Although the problem of anonymity will be mitigated if a password is used for user specific information, the load which memorizes a password is given to a user. Moreover, since it cannot prevent that a user makes a password reveal intentionally, there is also a trouble that the risk of unjust use will

increase.

[0009] The 2nd conventional technique is the approach of not giving an opportunity copying a ticket to persons other than a publisher as is shown in JP,8-147500,A. By this approach, both the device which prevents from copying the ticket in which the user is doing maintenance management, and the device which a ticket does not reveal from the communication link at the time of issue and verification are needed.

[0010] However, by this approach, since persons other than (1) publisher also carry out the contents of the communication link at the time of issue of (2) tickets with which it becomes difficult to prove the justification of a ticket for a third person since a ticket cannot be copied, and verification to secrecy, the trouble that it cannot prove not infringing on the right of users, such as privacy, at the time of issue of a ticket and verification arises.

[0011] The 3rd conventional technique is the approach which corrected the 2nd conventional technique so that the communication link at the time of verification can be exhibited, as shown in JP,6-52518,B. Although it records that it cannot copy to the equipment (certification equipment) which a user possesses by making a ticket into confidential information like the 2nd conventional technique by this approach, the approaches of verification differ. First, the verification equipment which verifies sends values (challenge) by which repeat use is not carried out, such as a random number, to certification equipment. Certification equipment performs the operation using the confidential information which is a ticket to a challenge, and returns the acquired value (response) to verification equipment. Verification equipment is checking what the response's calculated using confidential information and a challenge, and attests a user's justification. It becomes unnecessary to let a challenge and a response be secret communication by making it difficult in computational complexity to ask for confidential information conversely from a response.

[0012] This approach is used for authentication and information is not transmitted [whether the just ticket is held and] to except. For this reason, an expiration date etc. cannot be shown but only a simple ticket can be expressed. Moreover, there was a problem that it could not prove that the method of transmitting a ticket to certification equipment needs to carry out by secret communication link like the 2nd conventional technique, discloses a user's information unfairly, and is not infringing on a user's right.

[0013] Thus, each Prior art had a problem in the point at the sacrifice of the function of a ticket of contents certification and a user's anonymity to a third person, in order to realize the function to prevent unjust use required for a ticket.

[0014] [Related technique] The approach shown in Japanese Patent Application No. No. (un-opening [July 14, Heisei 9,] to the public) 188064 [nine to] is proposed as a related technique which solves these problems.

[0015] The general Challenge Handshake Authentication Protocol of this related technique is shown in drawing 1 . This protocol is a protocol which performs bidirectional authentication, and when both sides check the signature to authentication information (generated random number), it attests each other justification. Informational safe transfer is enabled by including a message (m, mu) in a part of mutual authentication information (random number).

[0016] The protocol of a related technique is explained with reference to drawing 1 . In drawing 1 , first, verification equipment generates the authentication information C based on a random number (S11), and this authentication information C is sent to certification equipment (S12). On the other hand, certification equipment generates another authentication information chi based on a random number, and sends the authentication information chi to verification equipment (S13, S14). Corresponding to a ticket, there is an internal state which cannot be operated in certification equipment from the exterior, and it can rewrite only by the response indication from verification equipment. The response indication in which the information (mu) to which modification of an internal state is permitted was included is created to a part of chi, verification equipment signs it, and verification equipment is sent to it at certification equipment (S15, S16). By checking the signature of a response indication rho, a transmitting person checks that it is just verification equipment, and, as for certification equipment, checks the rightness of

the information μ on internal-state modification with it (S17). The internal state of certification equipment is changed only into a right case for ρ according to the contents of μ (S18). The service set to verification equipment by performing a signature it being possible to restore D (S19) and according to D to the certification information R at the last when delivery (S20, S21) and verification equipment checked the signature is offered from Ticket t and the certification equipment proper information μ that certification equipment was created justly (S22, S23).

[0017] According to this approach, since the verification information on a ticket is public presentation, verification of a ticket is possible for it also to the 3rd person, and since a user does not have the need of showing the information which specifies a user at the time of verification of a ticket, anonymity is also kept.

[0018] Moreover, when verification equipment and certification equipment share each of each other's confidential information and public information and carry out mutual authentication, the problem of forgery of certification equipment and verification equipment is solved. Furthermore, by embedding information transmitting to a part of authentication information used for this certification, signal transduction verification equipment and between certification equipment is also made possible, and the contents of the ticket can be proved.

[0019] Thus, if the approach of this related technique is used, the safe electronic ticket which filled all the fundamental functions of an electronic ticket can be realized, and it is possible to solve all the above-mentioned problems.

[0020] By the way, with the previous related technique, it is premised on the ticket which verification equipment tends to verify becoming settled uniquely in certification equipment by sending the information as which verification equipment specifies a ticket to certification equipment. However, it is also considered in fact that two or more tickets verifiable [with the verification equipment] exist in certification equipment. For example, when a thing like the ticket of a railroad is considered, two or more tickets, such as a valid coupon ticket, a valid commuter pass, etc., may exist in certification equipment from the station. In such a case, with certification equipment, it cannot judge which ticket the user is going to use. Then, the need of choosing the ticket which a user uses beforehand in such cases arises.

[0021] And in such a scene, if a previous related technique is applied, the problem that it will be created and the response indication to which modification of the internal state corresponding to a ticket is permitted will be sent, without checking the contents of the ticket chosen and shown will arise.

[0022] This means that the internal state of the ticket which is not meant will be changed, when the ticket which the user mistook has been chosen.

[0023] Moreover, considering the case where it applies to the ticket of a railroad, it is possible by leaving record of entrance and checking record of entrance as an internal state, at the time of participation to prevent a malfeasance like cheating on the fare.

[0024] Here, a case so that it may leave only the fact of having only come in to the internal state corresponding to a ticket, as information on entrance is considered. In such a case, if it sends to certification equipment, without checking the modification authorization information on an internal state, and the contents of the ticket specifically shown entrance information, originally it will become possible to leave the fact of having come in at the station also to the ticket which cannot come in. If the entrance record over the ticket from the station near [station / which actually came in] the purpose station will forge supposing it can get the certification equipment holding the ticket with which it is the phase where of entrance was refused and the internal state was rewritten, although entrance with the ticket which is not just cannot be performed in fact, it is showing a ticket with the entrance record forged at the time of participation, and a cheating-on-the-fare action will become possible.

[0025] Thus, when a user chooses himself the ticket which it is going to prove, verification equipment needs to check that the shown ticket can verify justly with the verification equipment, before creating the authorization information which changes an internal state.

[0026] However, in a previous related technique, in order that such a check might not accomplish, there was a trouble that rewrote the internal state corresponding to the ticket which a user does not mean

accidentally, or the injustice by rewriting an internal state was possible.

[0027]

[Problem(s) to be Solved by the Invention] It aims at realizing an electronic ticket system by which verifying and verifying only the ticket which can verify verification equipment does not generate the information to which modification of an internal state is permitted to the ticket which is not right in this invention in order to solve the above-mentioned problem.

[0028]

[Means for Solving the Problem] In order to solve the above-mentioned technical problem, the electronic ticket system concerning this invention It consists of ticket verification equipment and certification equipment. Ticket verification equipment A ticket judging means to judge whether the ticket to verify can verify with verification equipment based on the ticket judging information which certification equipment presents, It has a dialogue verification means to verify whether certification equipment has computed ticket confidential information. Certification equipment It has at least the certification equipment proper information maintenance means, the ticket maintenance means, and a dialogue certification means by which the knowledge about ticket confidential information can be proved, from certification equipment proper information and a ticket.

[0029] In this configuration, verification equipment can check the compatibility of the ticket in certification equipment based on ticket judging information, and only when a right ticket is shown, the internal state of certification equipment can be changed.

[0030]

[The mode of implementation of invention] Hereafter, this invention is explained to a detail.

[0031] The electronic ticket structure-of-a-system Fig. of the example 1 of this invention is shown in [example 1] drawing 2. In drawing 2, the electronic ticket system shown in this example consists of verification equipment (it is also called a verification machine) 100, certification equipment (it is also called a certification machine) 200, and ticket assignment equipment 300.

[0032] Verification equipment 100 is constituted including the ticket judging section 101 which judges the justification of the ticket to verify, the authentication information generation section 102, the certification information generation section 103, the certification information verification section 104, the verification equipment privilege information attaching part 105, and the communications department 106.

[0033] On the other hand, certification equipment 200 is constituted including the certification equipment proper information attaching part 201, the ticket attaching part 202, the ticket judging information generation section 203, the authentication information generation section 204, the certification information verification section 205, the certification information generation section 206, the internal-state control section 207, and the communications department 208. In addition, the certification information generation section 103 of verification equipment 100 and the certification information generation section 206 of authentication equipment 200 possess the storage section holding the authentication information sent from authentication equipment 200 and verification equipment 100, respectively.

[0034] Moreover, a ticket and the ticket use information corresponding to each ticket are saved at the ticket attaching part 202. Moreover, the internal-state storage region corresponding to each ticket is secured to the ticket attaching part 202.

[0035] Here, certification equipment 200 is constituted by medium like an IC card with it difficult [to observe internal data and processing procedure from the outside].

[0036] Moreover, in this example, Ticket t is published as follows.

[0037]

[Table 1]

Ticket: $t = D \cdot F(n, L, du)$

D: the confidential information n:ticket method of a ticket private key du:certification equipment proper -- several F:un-colliding nature one-way function L:ticket use information, however $ED^{**}1 \bmod n$ -- it is E:ticket public key here. Ticket confidential information is D and ticket public information is E, n, and

L. F is realizable with a general Hash Function. Moreover, the information on the conditions using the ticket, for example, an expiration date, the location which can receive service goes into the ticket use information L.

[0038] The outline of the Challenge Handshake Authentication Protocol of this invention is shown in drawing 3. First, after a user specifies the ticket to be used from now on as certification equipment 200 with ticket assignment equipment 300, Challenge Handshake Authentication Protocol is started between verification equipment 100 and certification equipment 200.

[0039] In drawing 3, by Challenge Handshake Authentication Protocol, first, the authentication information generation section 102 of verification equipment 100 generates a random number C as authentication information, and sends to certification equipment 200 (S31, S32).

[0040] The certification equipment 200 which received authentication information performs ticket certification information generation processing (S33).

[0041] The flow chart of ticket certification information generation processing (S33) is shown in drawing 4. In drawing 4, the certification information generation section 206 of certification equipment 200 computes first the private key D used for a signature by the following count from the certification equipment proper information du saved at Ticket t, the ticket use information L, and the certification equipment proper information attaching part 201 (S41).

[0042]

[Equation 7]

$t + F(n, L, du)$

$= D - F(n, L, du) + F(n, L, du)$

= Generate the ticket judging information M to show that D, next the ticket judging information generation section 203 hold the right ticket from the ticket use information on the ticket attaching part 202, and the information on an internal-state storage region (S42). The certification information generation section 206 connects the ticket judging information M with the low order of the bit string of the authentication information C (S43), and is the ticket certification information T [0043]

[Equation 8] $T = (C || M) D \bmod \text{Count of } n$ generates (in addition, S44 and connecting notation || with a bit string are shown). In addition, besides the above-mentioned count, it is [0044].

[Equation 9]

$T = (C || M) t(C || M) F(n, L, du) \bmod$ The certification information T may be calculated by n.

[0045] Moreover, the authentication information generation section 204 generates a random number chi, and is taken as the 2nd authentication information (S44).

[0046] The ticket certification information T and the 2nd authentication information chi are sent to verification equipment 100 by the communications department 208 (S34). Ticket certification information is a right thing and it signs for guaranteeing that certification equipment and ticket judging information are not forged.

[0047] The verification equipment 100 which received T and chi performs ticket judging processing (S35 of drawing 3).

[0048] The flow chart of ticket judging processing (S35 of drawing 3) is shown in drawing 5. It is

[0049] from the ticket certification information T that the certification information verification section 104 of verification equipment 100 was sent in drawing 5, and the ticket public information E which the certification information verification section holds.

[Equation 10] $TE \bmod$ The value of n is calculated and it checks whether the part of the high order bit connected among the bit string is in agreement with the authentication information C (S51). When in agreement, the ticket judging information M is extracted further (S52). Next, the ticket judging section 101 judges whether it is what the internal state related with the ticket and the ticket based on the contents of M may verify with this verification equipment (S53). When this ticket may be verified as a result of a judgment, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200, and connects it with the low order of chi (S54, S55). Furthermore, the value rho which signed using the confidential information delta showing the privilege of verification equipment is created to this value (S56). Created rho is sent to

certification equipment 200 by the communications department 106 (S36).

[0050] On the other hand, when ticket certification information is not a right thing, or in being what a ticket should not verify, it ends a protocol (S57).

[0051] Next, the certification equipment which received rho performs internal-state modification processing (S37 of drawing 3).

[0052] The flow chart of internal-state modification processing (S37 of drawing 3) is shown in drawing 6. To the 2nd certification information rho that the certification information verification section 205 of certification equipment 200 was sent in drawing 6, the public information epsilon which checks the privilege of the verification equipment 100 which self holds is used, and it is [0053].

[Equation 11]

$$\rho^* \text{ mod } \nu$$

It calculates and checks whether the part of a high order is in agreement with the 2nd authentication information chi among the bit string (S61). As a result of a check, when it becomes clear that it is not right, a protocol is ended to a case (S62). Connected mu is extracted when it is able to be checked that it is a right thing (S63). The internal-state control section 207 changes the internal state of certification equipment 200 according to the contents of mu, and makes the result M' (S64, S65). The certification information generation section 206 is [0054] after connecting the value of M' with the bit string of the authentication information C.

[Equation 12] $R = (C || M') \text{ D mod Count of } n$ generates the certification information R (S66, S67). R is sent to verification equipment 100 by the communications department 208 (S38).

[0055] The verification equipment 100 which received R performs certification information verification processing (S39 of drawing 3).

[0056] The flow chart of certification information verification processing (S39 of drawing 3) is shown in drawing 7. The ticket public information E which the certification information verification section 104 of verification equipment 100 holds in drawing 7 is used, and it is [0057].

[Equation 13] RE mod The value of n is calculated and the bit string of the high order except M' connected as a result checks that it is in agreement with the authentication information C which verification equipment 100 generated first (S71). The defined service is offered, when it checks whether the contents of information M' which expresses the modification result of an internal state further are in agreement with the information mu to which internal-state modification sent as 2nd certification information rho is permitted when it is able to check (S72, S73, S74) and a check is completed (S75). When one of checks goes wrong, a protocol is completed and offer of service is not performed (S71, S74, S76).

[0058] The example 2 of [example 2] this invention is the case where an example 1 is realized as a ticket of the ticket of a railroad. The protocol at the time of entrance of a ticket is explained especially here.

[0059] Although the configuration of the example of this invention and the generation method of a ticket are the same as that of an example 1, verification equipment 100 is specifically an automatic ticket gate, and certification equipment 200 is a token like an IC card which can hold a ticket. And verification according to an automatic wicket in entrance and participation shall be performed, and the storage region corresponding to entrance or participation shall be secured to an internal state.

[0060] Below, the example of the ticket on Yokohama - Narita Airport July 18, 1997 explains. In addition, the step to which drawing 3 corresponds is pointed out suitably.

[0061] The ticket use information L on a ticket becomes like drawing 9. The ticket is registered into certification equipment 200 and the corresponding internal-state storage region is secured. The internal state before entrance is shown in drawing 8. Here, Ticket ID shows the ticket to be used from now on to 00005.

[0062] First, the authentication at the time of entrance is explained. Verification equipment 100 sends the information showing being entrance to certification equipment 200 with the authentication information C first (S32).

[0063] Certification equipment 200 generates the ticket judging information M. The contents of M are

shown in drawing 10 . As shown in drawing, the contents included in ticket use information and the contents of entrance / participation record of an internal state to show a busy condition are included in the ticket judging information M. The certification information generation section 206 connects M with C, performs the signature by the ticket private key D, and sends it to verification equipment 100 with the 2nd generated authentication information chi as ticket certification information T (S34).

[0064] Verification equipment 100 verifies ticket certification information, and checks the contents of the ticket judging information M further. Here, since an entrance station is within an expiration date and is an intact ticket at the Yokohama station, it is judged with it being the ticket which may carry out authentication here (S35).

[0065] Then, the information mu for changing the internal state of certification equipment 200 is created. The contents of mu are shown in drawing 11 . An entrance name of the station and time amount are recorded on mu. The certification information generation section 103 connects with the 2nd authentication information chi mu generated in this way, generates the value rho which performed the signature using the privilege information delta on verification equipment 100, and sends it to certification equipment 200 (S36).

[0066] The value of rho to which the certification information verification section 205 of certification equipment 200 was sent checks whether it is in agreement with the authentication information chi. When it is able to be checked that it is a right thing, the internal-state control section 207 changes the internal state of certification equipment 200 according to the contents of mu (S37). The situation of the internal state after modification is shown in drawing 12 . It turns out that the station and time amount of entrance were recorded. Next, the internal-state control section 207 makes M' the contents of modification of this internal state, i.e., entrance record. Like an example 1, the certification information generation section 206 connects the value of M' with the bit string of authentication information, generates the value R which performed the signature by ticket confidential information, and sends it to verification equipment 100 as certification information R (S38).

[0067] When the value of the certification information R is verified and the value is in agreement with the authentication information C, verification equipment 100 checks M', as a result of changing an internal state further. If M' corresponds with what was specified by mu, it will be judged as that by which the internal state was changed correctly, and the gate of a ticket gate machine will be opened.

[0068] Next, the authentication at the time of participation is explained. Although the authentication at the time of participation is the same as that of the time of entrance almost, the contents of the message told mutually differ.

[0069] Verification equipment 100 sends the information showing being participation to certification equipment with the authentication information C first (S32).

[0070] The ticket judging information generation section 203 of certification equipment 200 generates the ticket judging information M. The contents of M at the time of participation are shown in drawing 13 . The certification information generation section 206 connects M with C, performs the signature by the ticket private key D, and is taken as the ticket certification information T. And the 2nd authentication information chi which carried out authentication information generation section generation with the certification information T is sent to verification equipment (S34).

[0071] The certification information verification section 104 of verification equipment 100 verifies ticket certification information. In a verification result [of a ticket], or right case, the ticket judging section 101 checks the contents of the ticket judging information M. Here, since an entrance station is effective entrance record and is within the shelf-life of participation at the Yokohama station, it is judged with it being the ticket which can attest participation here (S35).

[0072] Next, the certification information generation section 103 creates the information mu for changing the internal state of certification equipment 200. The contents of mu are shown in drawing 14 . A participation name of the station and participation time amount are recorded on mu. The certification information generation section 103 connects generated mu with chi further, and generates the value rho which performed the signature using the privilege information delta on verification equipment. rho is sent to certification equipment 200 (S36).

[0073] The value of rho to which the certification information verification section 205 of certification equipment 200 was sent checks whether it is in agreement with the authentication information chi. When the right thing is able to be checked, according to the contents of mu, the internal-state control section 207 changes the internal state of certification equipment 200, and makes it M' as a result of [this] modification (i.e., participation record). The situation of the internal state after modification is shown in drawing 15 . A participation station and time amount are recorded. The certification information generation section 206 connects participation record M' with the bit string of the authentication information C, generates the certification information R which performed the signature by ticket confidential information, and sends it to verification equipment 100 (S38).

[0074] When the value of R is verified and the value is in agreement with the authentication information C, the certification information verification section 104 of verification equipment 200 checks M', as a result of changing an internal state further. If M' corresponds with what was specified with the value of mu, it will be judged as that by which the internal state was changed correctly, participation will be permitted, and the gate of a ticket gate machine will be opened (S39).

[0075] The [example 3] example 3 shows how to realize a gestalt like a coupon ticket.

[0076] Fundamentally, the configuration of this example, the generation method of a ticket, and the flow of the whole processing are the same as that of an example 1. The configuration of whole this example is shown in drawing 16 . It differs in that counter 202a which shows the remaining frequency of a coupon ticket is installed in the internal state as a description of this example. In drawing 16 , the sign corresponding to drawing 2 and a corresponding part was attached.

[0077] A user will register with certification equipment 200 first, if a coupon ticket is purchased. The internal-state storage region corresponding to a coupon ticket is secured at the time of registration, and the remaining use counts are written in counter 202a in it.

[0078] After a user specifies a coupon ticket with ticket assignment equipment 300 as a ticket used to certification equipment 200 after this, Challenge Handshake Authentication Protocol is started by the utilization time of a coupon ticket between verification equipment 100 and certification equipment 200.

[0079] At Challenge Handshake Authentication Protocol, it is the same as that of an example 1 till the place where verification equipment 100 generates a random number C as authentication information at, and delivery and certification equipment 200 calculate a ticket private key to certification equipment 200.

[0080] The flow chart of ticket certification information generation processing (it corresponds to S33 of drawing 3) of this example is shown in drawing 17 . In drawing 17 , the ticket judging information generation section 203 of certification equipment 200 extracts the count of the remainder of the internal state corresponding to the ticket of this coupon ticket, and records it on the ticket judging information M with ticket use information (S81-S84). And like an example 1, the certification information generation section 206 generates the ticket certification information T (S85), and the authentication information generation section 204 generates the 2nd authentication information chi (S86). T and chi are sent to verification equipment 100 by the communications department 208 (S34).

[0081] The verification equipment 100 which received T and chi performs ticket judging processing (it is ***** to S35 of drawing 3).

[0082] The flow chart of ticket judging processing is shown in drawing 18 . In drawing 18 , the certification information verification section 104 of verification equipment 100 verifies the received ticket certification information (S91). Ticket certification information extracts the ticket judging information M from ticket certification information to a right case (S92). The count of the remainder of a coupon ticket is recorded on the ticket judging information M. With [that value] one [or more], the ticket judging section 101 judges that this coupon ticket is still usable (S93). Furthermore, when the ticket judging section 101 also judges [that it is verifiable with this verification equipment 100 and] the contents of the ticket use information L, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200 (S94, S95). The contents which direct to reduce the use count of a coupon ticket by one as contents of mu are included. And by the same approach as an example 1, the 2nd certification information rho is created

using mu (S96, S97), and it sends to certification equipment 200 (S36).

[0083] Error processing is performed when verification and a ticket judging go wrong (S98).

[0084] The certification equipment 200 which received rho performs internal-state modification processing (it corresponds to S37 of [drawing 3](#)).

[0085] The flow chart of internal-state modification processing is shown in [drawing 19](#). In [drawing 19](#), the certification information verification section 205 of certification equipment 200 verifies the 2nd sent certification information rho (S101). When it is able to be checked that it is a right thing, according to the contents of mu, an internal-state control section reduces the remaining use count of a coupon ticket by one, and makes the result M' (S102-S104). The rest is the same approach as an example 1, and certification equipment 200 generates the certification information R, and sends it to verification equipment 100 (S105, S106). Error processing is performed when verification goes wrong at step S101 (S107).

[0086] Actuation of the subsequent verification equipments 100 is the same as that of an example 1, verifies the value of R and offers service.

[0087] In the example 4 of [example 4] this invention, although the whole configuration is the same as that of an example 1, the authentication approaches of ticket public information and ticket confidential information, or a ticket differ.

[0088] this example -- p -- the prime factor -- it is -- G -- dispersion -- a logarithm -- a finite group with a difficult problem -- it is -- g -- the origin of the order p of a finite group G -- it is -- [0089]

[Equation 14] $y = gx \bmod p$ When p is filled, (p, G, g, y) are ticket public information, and make x ticket confidential information. (p, G, g) can also be made common by the whole system.

[0090] At this time, a ticket is [0091] from the ticket description information x, the certification equipment proper information du, the ticket use information L, and the information p that specifies a group.

[Equation 15] $t = x - F(du, L, y, p)$

It is calculated by carrying out. Here, F is the one-way function of un-colliding nature, and a general Hash Function can realize it. L is the same ticket use information as an example 1.

[0092] Moreover, the above (p, G, g) is [0093] as common as a thing showing the privilege of verification equipment.

[Equation 16]

$$\eta = g^{\epsilon} \bmod p$$

***** -- let eta [like] into public information and let xi be confidential information.

[0094] G can be constituted as a multiplicative group in fact, or it can constitute as an elliptic curve on finite field.

[0095] The outline of the Challenge Handshake Authentication Protocol of this invention is shown in [drawing 20](#).

[0096] First, after a user specifies the ticket to be used from now on to certification equipment, Challenge Handshake Authentication Protocol is started between verification equipment and certification equipment.

[0097] In [drawing 20](#), by this Challenge Handshake Authentication Protocol, first, the authentication information generation section 102 of verification equipment 100 generates a random number r, calculates $C = gr$, and sends to certification equipment by making this into authentication information (S201, S202, S203).

[0098] The certification equipment 200 which received the authentication information C performs ticket certification information generation processing (S204).

[0099] The flow chart of ticket certification information generation processing is shown in [drawing 21](#). In [drawing 21](#), the certification information generation section 206 of certification equipment 200 computes first the private key x used for a signature by the following count from p of Ticket t, the ticket use information L, and ticket public information, and the certification equipment proper information du (S211).

[0100]

[Equation 17]

 $t+F(y,L,du,p)$ $=x-F(y,L,du,p)+F(y,L,du,p)$

= Generate the ticket judging information M to show that x, next the ticket judging information generation section 203 hold the right ticket from the additional information L of a ticket, and the information on an internal state (S212). The certification information generation section 206 generates the following values as certification information (S213, S214).

[0101]

[Equation 18] $T = (C||M)$ and $Cx \bmod p$ -- in addition, the certification information T is calculable with the following formulas besides the above.

[0102]

[Equation 19]

$T = (C||M)$ and $CtCF(y, L, du, p) \bmod p$ and the authentication information generation section 204 generate random-number r' to coincidence, and are [0103].

[Equation 20] $Chi = gr' \bmod p$ is sent to verification equipment as 2nd authentication information (S215, S216, S205). The information included in the ticket judging information M is the same as that of examples 1-3.

[0104] The certification information T and the 2nd authentication information chi are sent to verification equipment 100 by the communications department 208.

[0105] The verification equipment 100 which received T and chi performs ticket judging processing (S206 of drawing 20).

[0106] The flow chart of ticket judging processing is shown in drawing 22. It is [0107] from the ticket certification information that the certification information verification section 103 of verification equipment 100 was sent in drawing 22.

[Equation 21] $T/yr \bmod p = (C||M)$ and $Cx/yr \bmod p$ The value of p is calculated and it checks whether parts other than M connected among the bit string are in agreement with the authentication information C (S221). When in agreement, the ticket judging section 101 judges further whether it is what the internal state related with the ticket and the ticket may verify with this verification equipment 100 from the contents of the ticket judging information M (S222, S223). When this ticket may be verified as a result of a judgment, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200, and connects it with chi (S224, S225). And the following values are generated as 2nd authentication information to this value using the confidential information xi showing the privilege of verification equipment (S226).

[0108]

[Equation 22]

$$\rho = (x || \mu) \cdot x^r \bmod p$$

rho is sent to certification equipment 200 by the communications department 106. On the other hand, when ticket certification information is not a right thing, or in being what a ticket should not verify, it ends a protocol (S227).

[0109] Next, the certification equipment 200 which received rho performs internal-state modification processing (S208 of drawing 20).

[0110] The flow chart of internal-state modification processing is shown in drawing 23. It is [0111] from a response indication to which the certification information verification section 205 of certification equipment 200 was sent in drawing 23.

[Equation 23]

$$\rho / \eta^{r'} \bmod p = (x || \mu) \cdot x^r / \eta^{r'} \bmod p$$

A ** value is calculated and it checks whether parts other than mu connected among the bit string are in agreement with the 2nd authentication information chi (S231). When it is able to be checked that it is a

right thing, according to the information the internal-state control section 207 instructs modification of the internal state of mu to be, the internal state of certification equipment 200 changes and the result is made into M' (S232-S234). On the other hand, as a result of a check, when it becomes clear that it is not right, a protocol is ended to a case (S137).

[0112] after the certification information generation section 206 connects the value of M' with the bit string of the authentication information C -- the following values -- certification information -- ** -- it generates by carrying out (S235, S236).

[0113]

[Equation 24] $R = (C || M')$ and $Cx \bmod p$ -- the certification information R generated in this way is sent to verification equipment 100 by the communications department 208 (S209).

[0114] The verification equipment 100 which received R performs certification information verification processing S210 (drawing 20).

[0115] The flow chart of certification information verification processing is shown in drawing 24 . It is [0116] from the ticket certification information that the certification information verification section 104 was sent in drawing 24 .

[Equation 25] $R/yr \bmod p$ The value of $p = (C || M')$ and $Cx/yr \bmod p$ is calculated and, as a result, the bit string of the high order except M' checks that it is in agreement with the authentication information C which verification equipment 100 generated first (S241). The defined service is offered, when it checks whether the contents of information M' which expresses the modification result of an internal state further are in agreement with the information mu to which internal-state modification sent as 2nd certification information rho is permitted when it is able to check (S242, S243, S244) and a check is completed (S245). When one of checks goes wrong, a protocol is completed and offer of service is not performed (S246).

[0117]

[Effect of the Invention] As explained above, according to this invention, an electronic ticket system by which verifying and verifying only the ticket which can verify verification equipment does not generate the information to which modification of an internal state is permitted to the ticket which is not right can be realized, and the malfeasance by modification of the internal state which a user does not mean, and modification of an internal state can be prevented.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] It is the electronic ticket system which has certification equipment and verification equipment and verifies owning the ticket with the above-mentioned just certification equipment. The above-mentioned certification equipment A certification equipment proper information maintenance means to hold the proper information on the above-mentioned certification equipment, and a ticket maintenance means to hold the above-mentioned ticket, The ticket judging information generation section which generates the ticket judging information that the contents of a right of the above-mentioned ticket or the busy condition of the above-mentioned ticket is expressed, Ticket confidential information is generated from the above-mentioned certification equipment proper information and the above-mentioned ticket at least. It has a certification information generation means to generate certification information using the above-mentioned ticket confidential information. The above-mentioned verification equipment A ticket judging means to judge whether I may perform verification processing based on the above-mentioned ticket judging information which the above-mentioned certification equipment presents, The electronic ticket system characterized by having a certification information verification means to verify whether the above-mentioned certification equipment has generated ticket confidential information based on the above-mentioned certification information.

[Claim 2] It is the electronic ticket system are an electronic ticket system according to claim 1, the above-mentioned verification equipment has an authentication information generation means to generate the authentication information used by dialogue certification, and the certification information generation means of the above-mentioned certification equipment generates the above-mentioned certification information using the authentication information which the above-mentioned verification equipment generated.

[Claim 3] It is the electronic ticket system which transmits the ticket judging information on a ticket that it is an electronic ticket system according to claim 2, and the above-mentioned certification equipment and the above-mentioned verification equipment have means of communications, and it is going to prove the above-mentioned certification equipment to the above-mentioned verification equipment.

[Claim 4] They are claim 2 thru/or an electronic ticket system given in 3. The above-mentioned electronic ticket system The above-mentioned verification equipment and the above-mentioned certification equipment are resembled, in addition it has ticket issue equipment. The above-mentioned ticket issue equipment A ticket description information maintenance means to hold the above-mentioned ticket confidential information which is the secret description information on the ticket to publish, and corresponding ticket public information, A certification equipment proper information maintenance means for ticket issue to hold the proper information on the above-mentioned certification equipment which a user holds, The electronic ticket system which has ticket issue ***** which creates the ticket which is digital information using the above-mentioned ticket confidential information currently held for the above-mentioned ticket description information maintenance means, and the above-mentioned certification equipment proper information maintenance means for the above-mentioned certification equipment proper information maintenance means for ticket issue.

[Claim 5] It is the electronic ticket system are claim 2 thru/or the electronic ticket system of 4, and the certification information generation means of the above-mentioned certification equipment is a predetermined approach, and calculates the ticket certification information use to the judgment of the above-mentioned ticket judging means as one of the above-mentioned certification information, from the authentication information sent from the above-mentioned verification equipment at least, the above-mentioned ticket, the above-mentioned ticket judging information, and the above-mentioned certification equipment proper information.

[Claim 6] It is the electronic ticket system which are an electronic ticket system according to claim 5, and the above-mentioned certification equipment makes the ticket use information that the use conditions of a ticket were defined correspond with a ticket, and holds to the above-mentioned ticket attaching part.

[Claim 7] It is the electronic ticket system which uses the above-mentioned ticket use information at least in case it is an electronic ticket system according to claim 5 and the above-mentioned certification equipment creates the above-mentioned ticket judging information.

[Claim 8] It is the electronic ticket system which is an electronic ticket system according to claim 6, and is equipped with the internal-state storage region holding a strange internal state with the above-mentioned good certification equipment, and the internal-state control means which controls the value of the above-mentioned internal state.

[Claim 9] It is the electronic ticket system which uses the information on the internal-state storage region of the above-mentioned certification equipment at least in case it is an electronic ticket system according to claim 8 and the ticket judging information generation means of the above-mentioned certification equipment creates the above-mentioned ticket judging information.

[Claim 10] It rewrites from the outside and at least the part of the strange good internal states which are claim 8 thru/or the electronic ticket system of 9, and the internal-state storage region of the above-mentioned certification equipment holds is a impossible electronic ticket system.

[Claim 11] It is the electronic ticket system by which it is claim 8 thru/or the electronic ticket system of 10, and the certification information generation means of the above-mentioned certification equipment calculates the above-mentioned certification information at least using the above-mentioned ticket, the above-mentioned ticket use information, and the above-mentioned certification equipment proper information.

[Claim 12] It is the electronic ticket system are claim 8 thru/or the electronic ticket system of 11, and above-mentioned certification equipment has the authentication information maintenance means hold the above-mentioned authentication information sent from the above-mentioned verification means, and the above-mentioned certification information generation means changes the authentication information currently held at the above-mentioned authentication information maintenance means using the ticket judging information generated by the above-mentioned ticket judging information generation means, and use to generation of the above-mentioned certification information.

[Claim 13] When ticket judging information which is the electronic ticket system of claim 12 and the above-mentioned ticket judging information generation means generated is set to M and the above-mentioned authentication information sets to C, the certification information generation means of the above-mentioned certification equipment is the electronic ticket system which updates to what joined M to C in the authentication information C currently held at the above-mentioned authentication information maintenance means.

[Claim 14] They are claim 12 thru/or the electronic ticket system of 13. The certification information generation means of the above-mentioned certification equipment It is possible to generate ticket certification information as one of the above-mentioned certification information. The above-mentioned ticket certification information The electronic ticket system generated by calculating ticket confidential information by the predetermined approach from the above-mentioned ticket, the above-mentioned ticket use information, and the above-mentioned certification equipment proper information, and performing count using ticket confidential information to the above-mentioned authentication information.

[Claim 15] It is the electronic ticket system of claim 14, p and q are the prime factors, and it is $n=p \cdot q$, and is $DE^{**}1 \cdot \text{mod } (p-1)(q-1)$ When relation is filled, The above-mentioned ticket confidential information is D, ticket public information is (n, E), the above-mentioned ticket use information is L, the above-mentioned certification equipment proper information is the secret value du, and, on the other hand, $f(du, L, n)$ is made into a tropism function. When the ticket is given by $t=D \cdot f(du, L, n)$, the certification information generation means of the above-mentioned certification equipment As opposed to the above-mentioned authentication information C (authentication information which the above-mentioned certification information generation means changed) the law of C -- the power by t in n, and the law of C -- law with the power in n according to the tropism function value f(du, L, n) on the other hand -- product $CtCf$ in n (du, L, n) mod Electronic ticket system which calculates ticket certification information as n.

[Claim 16] It is the electronic ticket system of claim 14, p and q are the prime factors, and it is $n=p \cdot q$, and is $DE^{**}1 \cdot \text{mod } (p-1)(q-1)$ When relation is filled, The above-mentioned ticket confidential information is D, ticket public information is (n, E), the above-mentioned ticket use information is L, the above-mentioned certification equipment proper information is the secret value du, and, on the other hand, $f(du, L, n)$ is made into a tropism function. When the above-mentioned ticket is given by $t=D \cdot f(du, L, n)$, the above-mentioned certification equipment $t+f(du, L, n)=D$ is calculated beforehand, the value is used, and it is $T=CD$ to the above-mentioned authentication information C (authentication information which the above-mentioned certification information generation means changed) mod Electronic ticket system which calculates the ticket certification information T as n.

[Claim 17] the electronic ticket system of claim 14 -- it is -- g -- dispersion -- a logarithm -- the primitive root of a group with a difficult problem -- it is -- p -- the prime factor -- it is -- an integer x -- receiving -- $y=gx \text{ mod } n$ When p is realized The above-mentioned ticket confidential information is x, ticket public information is (y, p, g), the above-mentioned ticket use information is L, the above-mentioned certification equipment proper information is the secret value du, and, on the other hand, $f(du, L, y)$ is made into a tropism function. When the above-mentioned ticket is given by $t=x \cdot f(du, L, y)$, the above-mentioned certification equipment As opposed to the above-mentioned authentication information C (authentication information which the above-mentioned certification information generation means changed) the above-mentioned ticket judging information T -- the law of C -- the power by t in p, and the law of C -- law with the power in p which, on the other hand, makes a characteristic the tropism function value f(du, L, y) -- product $CtCf$ in p (du, L, y) Electronic ticket system which calculates the above-mentioned certification information as mod n.

[Claim 18] the electronic ticket system of claim 14 -- it is -- g -- dispersion -- a logarithm -- the primitive root of a group with a difficult problem -- it is -- p -- the prime factor -- it is -- an integer x -- receiving -- $y=gx \text{ mod } n$ When p is realized The above-mentioned ticket confidential information is x, ticket public information is (y, p, g), the above-mentioned ticket use information is L, the above-mentioned certification equipment proper information is the secret value du, and, on the other hand, $f(du, L, y)$ is made into a tropism function. When the above-mentioned ticket is given by $t=x \cdot f(du, L, y)$, the above-mentioned certification equipment It is Cx , in case $t+f(du, L, y)=x$ are calculated beforehand and the ticket (authentication information which above-mentioned certification information generation means changed) judging information T is calculated to the above-mentioned authentication information C. mod Electronic ticket system using the value of p.

[Claim 19] It is the electronic ticket system are claim 14 thru/or the electronic ticket system of 18, and the certification information verification means of the above-mentioned verification equipment verifies the justification of the above-mentioned ticket certification information from the authentication information which the above-mentioned authentication information generation means created, the ticket certification information which were sent from the above-mentioned certification equipment, and the above-mentioned ticket public information, and a right case derives the ticket judging information were embedded to the above-mentioned ticket certification information, in the above-mentioned ticket certification information.

[Claim 20] It is the electronic ticket system of claim 19, and the above-mentioned authentication

information is C. When the above-mentioned ticket certification information is T, it is the above-mentioned ticket public information (n, E) and there is certain bit string M, the certification information verification means of the above-mentioned verification equipment the above-mentioned ticket certification information T -- law -- the bit string which joined C and M for what carried out the exponentiation by E by n -- comparing -- $TE \bmod n$ If it is $n=C||M$ (notation || is junction of a bit string) It is the electronic ticket system by which the above-mentioned ticket certification information is judged to be the right, and the above-mentioned ticket certification information derives M as the above-mentioned ticket judging information in a right case.

[Claim 21] It is the electronic ticket system of claim 19, and the above-mentioned authentication information is C. When the above-mentioned ticket certification information is T and the above-mentioned ticket public information is (p, g, y), the certification information verification means of the above-mentioned verification equipment When setting to r the random number which self generated, there is certain bit string M, and it is $T/yr \bmod p = (C||M)$ (notation || is junction of a bit string) If it has become It is the electronic ticket system by which the above-mentioned ticket certification information is judged to be the right, and the above-mentioned ticket certification information derives M as ticket judging information in a right case.

[Claim 22] They are claim 8 thru/or the electronic ticket system of 21. The above-mentioned certification equipment 2nd authentication information generation means to generate the 2nd authentication information for attesting the above-mentioned verification equipment, It has the 2nd certification information verification means for verifying the 2nd certification information which the above-mentioned verification equipment generates. The certification information verification means of the above 2nd The certification information on the above 2nd is the electronic ticket system by which the certification information on the above 2nd verifies whether it is the right from the authentication information on the above 2nd, the certification information on the above 2nd, and ticket public information, and the above-mentioned internal-state control means changes the internal state of the above-mentioned certification equipment a right case.

[Claim 23] It is the electronic ticket system which determines whether are the electronic ticket system of claim 22 and the certification information verification means of the above-mentioned verification equipment generates the certification information on the above 2nd based on the result of the judgment by the above-mentioned ticket judging means.

[Claim 24] It is the electronic ticket system which it is the electronic ticket system of claim 22, and the above-mentioned certification equipment relates with a ticket the internal state which functions as a counter of a ticket, holds from the exterior to an internal-state storage region in the form which is not rewritable, and judges the certification information verification means of the above-mentioned verification equipment to be what has a corresponding ticket invalid when the value of the counter of the internal state included in the ticket judging information sent from the above-mentioned certification equipment is a predetermined value.

[Claim 25] It is claim 22 thru/or the electronic ticket system of 24, p' and q' are the prime factors, and it is $nu=p'-q'$, and is $\text{delta} \epsilon \pi^{*} 1 \bmod (p' - 1) (q' - 1)$ When relation is filled, for the 2nd certification information verification means of the above-mentioned certification equipment, the authentication information chi on the above 2nd and the certification information rho on the above 2nd are [Equation 1].

$$\chi = \rho^e \bmod \nu$$

The electronic ticket system which the certification information on the above 2nd judges to a ***** case to be the right.

[Claim 26] claim 22 thru/or the electronic ticket system of 24 -- it is -- g -- dispersion -- a logarithm -- the primitive root of a group with a difficult problem -- it is -- p -- the prime factor -- it is -- an integer xi -- receiving -- [Equation 2]

$$\eta = g^f \bmod p$$

***** -- suddenly -- coming -- alike -- the 2nd authentication information generation means of certification equipment -- random-number r and authentication information $chi = gr^r$ of the above 2nd -- generating -- the certification information verification means of the above 2nd -- the certification information ρ on the above 2nd -- $\rho = \text{etar} \bmod \text{*****}$ system which the certification information on the above 2nd judges to be the right when $p = chi$ is filled.

[Claim 27] The certification information on the above 2nd is the electronic ticket system by which the information which is the electronic ticket system of claim 22, and as for which the 2nd certification information verification means of the above-mentioned certification equipment was embedded by the right case to the certification information on the above 2nd is derived.

[Claim 28] It is the electronic ticket system which uses as information for being the electronic ticket system of claim 27 and permitting modification of the above-mentioned internal information for the information by which the 2nd certification information verification means of the above-mentioned certification equipment was drawn from the certification information on the above 2nd.

[Claim 29] It is claim 27 thru/or the electronic ticket system of 28, ticket public information contains μ and ϵ , and, for the 2nd certification information verification means of the above-mentioned certification equipment, the authentication information chi on the above 2nd and the certification information ρ on the above 2nd are [Equation 3] to certain bit string μ .

$\chi \mid \mid \mu = \rho^{\epsilon} \bmod \nu$ (記号 \mid はビット列の接合)

The electronic ticket system by which the certification information on the above 2nd judges with the right, and derives μ as information embedded to the certification information on the above 2nd at the time of *****.

[Claim 30] It is the electronic ticket system which changes the internal state which is the electronic ticket system of claim 27 and was held in the above-mentioned internal-state storage region based on the information by which the internal-state control means of the above-mentioned certification equipment was drawn from the certification information on the above 2nd.

[Claim 31] It is the electronic ticket system which judges whether it is the electronic ticket system of claim 30, and the certification information verification means of the above 2nd of the above-mentioned certification equipment generates the above-mentioned certification information correctly based on the information to which internal-state modification sent from the above-mentioned verification equipment is permitted, and an internal state.

[Claim 32] It is the electronic ticket system are claim 22 thru/or the electronic ticket system of 31, above-mentioned verification equipment has the verification equipment privilege information attaching part holding verification equipment privilege information which is the confidential information showing the privilege of the above-mentioned verification equipment, and the 2nd certification information generation section which generates the certification information on the above 2nd, and the certification information generation section of the above 2nd generates the 2nd certification information from the authentication information on the above 2nd, and above-mentioned verification equipment privilege information.

[Claim 33] When it is the electronic ticket system of claim 32, the above-mentioned verification equipment privilege information is set to δ and corresponding public information is set to (μ, ϵ) , the 2nd certification information generation section of the above-mentioned verification equipment is [Equation 4] about the certification information ρ on the above 2nd from the authentication information chi on the above 2nd.

$\rho = \chi^{\delta} \bmod \nu$

The electronic ticket system which generate by carrying out.

[Claim 34] It is the electronic ticket system of claim 32, and the above-mentioned verification equipment privilege information is set to ξ , corresponding public information is set to (p, g, eta) , and it is [Equation 5].

$\eta = g^{\xi} \bmod p$

The 2nd certification information generation section of the above-mentioned verification equipment is [as opposed to / when ***** is filled / the authentication information chi on the above 2nd] [Equation 6].

$$\chi^f \bmod p$$

The electronic ticket system which generates the certification information rho on the above 2nd using a ** value.

[Claim 35] It is the electronic ticket system are claim 32 thru/or the electronic ticket system of 34, and the above-mentioned verification equipment has the 2nd authentication information attaching part holding the authentication information on the above 2nd, and calculate the certification information on the above 2nd from the information grant a permission in modification of the internal state of certification equipment, and the authentication information on the above 2nd in case the 2nd certification information generation section of the above-mentioned verification equipment gives the count which used the above-mentioned verification equipment privilege information.

[Claim 36] It is the electronic ticket system which updates the authentication information on the above 2nd held at the authentication information attaching part of the above 2nd using the information to which modification of the internal state of the above-mentioned certification equipment is permitted before it is claim 32 thru/or the electronic ticket system of 34 and the 2nd certification information generation section of the above-mentioned verification equipment performs count which used the above-mentioned verification equipment privilege information.

[Claim 37] It is the electronic ticket system which updates to what was the electronic ticket system of claim 36, and joined mu for the 2nd authentication information held at the authentication information attaching part of the above 2nd at chi when the 2nd certification information generation section of the above-mentioned verification equipment set to mu information to which modification of the internal state of the above-mentioned certification equipment is permitted and authentication information on the above 2nd was set to chi.

[Claim 38] The electronic ticket system currently held in a defense means to be claim 1 thru/or an electronic ticket system given in 37, and to close at least that the above-mentioned certification equipment observes internal data and processing procedure from the outside if.

[Claim 39] The electronic ticket system by which it is a claim thru/or an electronic ticket system given in 37, and the above-mentioned certification equipment is constituted as a portable small arithmetic unit of an IC card etc. at least.

[Claim 40] It is the electronic ticket system which has certification equipment and verification equipment and verifies owning the ticket with the above-mentioned just certification equipment. The above-mentioned certification equipment A certification equipment proper information maintenance means to hold the proper information on the above-mentioned certification equipment, and a ticket maintenance means to hold the above-mentioned ticket, The ticket judging information generation section which generates the ticket judging information that the contents of a right of the above-mentioned ticket or the busy condition of the above-mentioned ticket is expressed, It has a certification information generation means to generate certification information from the above-mentioned certification equipment proper information and the above-mentioned ticket at least. The above-mentioned verification equipment A ticket judging means to judge whether I may perform verification processing based on the above-mentioned ticket judging information which the above-mentioned certification equipment presents, The electronic ticket system by which the above-mentioned certification equipment is characterized by having a certification information verification means to verify whether the above-mentioned certification information was generable from the above-mentioned certification equipment proper information and the above-mentioned ticket.

[Claim 41] In the electronic ticket use approach of performing service predetermined by the verification equipment side, performing mutual recognition between verification equipment and the authentication equipment holding an electronic ticket, and changing an internal state by the authentication equipment

side The step which shows the above-mentioned verification equipment the ticket judging information that the above-mentioned certification equipment expresses the contents of a right of the above-mentioned electronic ticket, or the busy condition of the above-mentioned electronic ticket, The electronic ticket use approach that the above-mentioned verification equipment is characterized by having the step which judges whether I may perform verification processing based on the shown above-mentioned ticket judging information.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention] This invention relates to the technique of creating a ticket and a card electronically and using them.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

PRIOR ART

[Background of the Invention]

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] As explained above, according to this invention, an electronic ticket system by which verifying and verifying only the ticket which can verify verification equipment does not generate the information to which modification of an internal state is permitted to the ticket which is not right can be realized, and the malfeasance by modification of the internal state which a user does not mean, and modification of an internal state can be prevented.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] It aims at realizing an electronic ticket system by which verifying and verifying only the ticket which can verify verification equipment does not generate the information to which modification of an internal state is permitted to the ticket which is not right in this invention in order to solve the above-mentioned problem.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] In order to solve the above-mentioned technical problem, the electronic ticket system concerning this invention It consists of ticket verification equipment and certification equipment. Ticket verification equipment A ticket judging means to judge whether the ticket to verify can verify with verification equipment based on the ticket judging information which certification equipment presents, It has a dialogue verification means to verify whether certification equipment has computed ticket confidential information. Certification equipment It has at least the certification equipment proper information maintenance means, the ticket maintenance means, and a dialogue certification means by which the knowledge about ticket confidential information can be proved, from certification equipment proper information and a ticket.

[0029] In this configuration, verification equipment can check the compatibility of the ticket in certification equipment based on ticket judging information, and only when a right ticket is shown, the internal state of certification equipment can be changed.

[0030]

[The mode of implementation of invention] Hereafter, this invention is explained to a detail.

[0031] The electronic ticket structure-of-a-system Fig. of the example 1 of this invention is shown in [example 1] drawing 2. In drawing 2, the electronic ticket system shown in this example consists of verification equipment (it is also called a verification machine) 100, certification equipment (it is also called a certification machine) 200, and ticket assignment equipment 300.

[0032] Verification equipment 100 is constituted including the ticket judging section 101 which judges the justification of the ticket to verify, the authentication information generation section 102, the certification information generation section 103, the certification information verification section 104, the verification equipment privilege information attaching part 105, and the communications department 106.

[0033] On the other hand, certification equipment 200 is constituted including the certification equipment proper information attaching part 201, the ticket attaching part 202, the ticket judging information generation section 203, the authentication information generation section 204, the certification information verification section 205, the certification information generation section 206, the internal-state control section 207, and the communications department 208. In addition, the certification information generation section 103 of verification equipment 100 and the certification information generation section 206 of authentication equipment 200 possess the storage section holding the authentication information sent from authentication equipment 200 and verification equipment 100, respectively.

[0034] Moreover, a ticket and the ticket use information corresponding to each ticket are saved at the ticket attaching part 202. Moreover, the internal-state storage region corresponding to each ticket is secured to the ticket attaching part 202.

[0035] Here, certification equipment 200 is constituted by medium like an IC card with it difficult [to observe internal data and processing procedure from the outside].

[0036] Moreover, in this example, Ticket t is published as follows.

[0037]

[Table 1]

Ticket: $t = D - F(n, L, du)$

D: the confidential information n:ticket method of a ticket private key du:certification equipment proper -- several F:un-colliding nature one-way function L:ticket use information, however $ED^{**} \bmod n$ -- it is E:ticket public key here. Ticket confidential information is D and ticket public information is E, n, and L. F is realizable with a general Hash Function. Moreover, the information on the conditions using the ticket, for example, an expiration date, the location which can receive service goes into the ticket use information L.

[0038] The outline of the Challenge Handshake Authentication Protocol of this invention is shown in drawing 3. First, after a user specifies the ticket to be used from now on as certification equipment 200 with ticket assignment equipment 300, Challenge Handshake Authentication Protocol is started between verification equipment 100 and certification equipment 200.

[0039] In drawing 3, by Challenge Handshake Authentication Protocol, first, the authentication information generation section 102 of verification equipment 100 generates a random number C as authentication information, and sends to certification equipment 200 (S31, S32).

[0040] The certification equipment 200 which received authentication information performs ticket certification information generation processing (S33).

[0041] The flow chart of ticket certification information generation processing (S33) is shown in drawing 4. In drawing 4, the certification information generation section 206 of certification equipment 200 computes first the private key D used for a signature by the following count from the certification equipment proper information du saved at Ticket t, the ticket use information L, and the certification equipment proper information attaching part 201 (S41).

[0042]

[Equation 7]

 $t + F(n, L, du)$ $= D - F(n, L, du) + F(n, L, du)$

= Generate the ticket judging information M to show that D, next the ticket judging information generation section 203 hold the right ticket from the ticket use information on the ticket attaching part 202, and the information on an internal-state storage region (S42). The certification information generation section 206 connects the ticket judging information M with the low order of the bit string of the authentication information C (S43), and is the ticket certification information T [0043]

[Equation 8] $T = (C || M) D \bmod \text{Count of } n$ generates (in addition, S44 and connecting notation || with a bit string are shown). In addition, besides the above-mentioned count, it is [0044].

[Equation 9]

 $T = (C || M) t (C || M) F(n, L, du) \bmod n$ The certification information T may be calculated by n.

[0045] Moreover, the authentication information generation section 204 generates a random number chi, and is taken as the 2nd authentication information (S44).

[0046] The ticket certification information T and the 2nd authentication information chi are sent to verification equipment 100 by the communications department 208 (S34). Ticket certification information is a right thing and it signs for guaranteeing that certification equipment and ticket judging information are not forged.

[0047] The verification equipment 100 which received T and chi performs ticket judging processing (S35 of drawing 3).

[0048] The flow chart of ticket judging processing (S35 of drawing 3) is shown in drawing 5. It is [0049] from the ticket certification information T that the certification information verification section 104 of verification equipment 100 was sent in drawing 5, and the ticket public information E which the certification information verification section holds.

[Equation 10] $TE \bmod n$ The value of n is calculated and it checks whether the part of the high order bit connected among the bit string is in agreement with the authentication information C (S51). When in agreement, the ticket judging information M is extracted further (S52). Next, the ticket judging section

101 judges whether it is what the internal state related with the ticket and the ticket based on the contents of M may verify with this verification equipment (S53). When this ticket may be verified as a result of a judgment, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200, and connects it with the low order of chi (S54, S55). Furthermore, the value rho which signed using the confidential information delta showing the privilege of verification equipment is created to this value (S56). Created rho is sent to certification equipment 200 by the communications department 106 (S36).

[0050] On the other hand, when ticket certification information is not a right thing, or in being what a ticket should not verify, it ends a protocol (S57).

[0051] Next, the certification equipment which received rho performs internal-state modification processing (S37 of drawing 3).

[0052] The flow chart of internal-state modification processing (S37 of drawing 3) is shown in drawing 6. To the 2nd certification information rho that the certification information verification section 205 of certification equipment 200 was sent in drawing 6, the public information epsilon which checks the privilege of the verification equipment 100 which self holds is used, and it is [0053].

[Equation 11]

$$\rho^e \bmod \nu$$

It calculates and checks whether the part of a high order is in agreement with the 2nd authentication information chi among the bit string (S61). As a result of a check, when it becomes clear that it is not right, a protocol is ended to a case (S62). Connected mu is extracted when it is able to be checked that it is a right thing (S63). The internal-state control section 207 changes the internal state of certification equipment 200 according to the contents of mu, and makes the result M' (S64, S65). The certification information generation section 206 is [0054] after connecting the value of M' with the bit string of the authentication information C.

[Equation 12] $R = (C \| M') D \bmod \text{Count of } n$ generates the certification information R (S66, S67). R is sent to verification equipment 100 by the communications department 208 (S38).

[0055] The verification equipment 100 which received R performs certification information verification processing (S39 of drawing 3).

[0056] The flow chart of certification information verification processing (S39 of drawing 3) is shown in drawing 7. The ticket public information E which the certification information verification section 104 of verification equipment 100 holds in drawing 7 is used, and it is [0057].

[Equation 13] $RE \bmod n$ The value of n is calculated and the bit string of the high order except M' connected as a result checks that it is in agreement with the authentication information C which verification equipment 100 generated first (S71). The defined service is offered, when it checks whether the contents of information M' which expresses the modification result of an internal state further are in agreement with the information mu to which internal-state modification sent as 2nd certification information rho is permitted when it is able to check (S72, S73, S74) and a check is completed (S75). When one of checks goes wrong, a protocol is completed and offer of service is not performed (S71, S74, S76).

[0058] The example 2 of [example 2] this invention is the case where an example 1 is realized as a ticket of the ticket of a railroad. The protocol at the time of entrance of a ticket is explained especially here.

[0059] Although the configuration of the example of this invention and the generation method of a ticket are the same as that of an example 1, verification equipment 100 is specifically an automatic ticket gate, and certification equipment 200 is a token like an IC card which can hold a ticket. And verification according to an automatic wicket in entrance and participation shall be performed, and the storage region corresponding to entrance or participation shall be secured to an internal state.

[0060] Below, the example of the ticket on Yokohama - Narita Airport July 18, 1997 explains. In addition, the step to which drawing 3 corresponds is pointed out suitably.

[0061] The ticket use information L on a ticket becomes like drawing 9. The ticket is registered into certification equipment 200 and the corresponding internal-state storage region is secured. The internal

state before entrance is shown in drawing 8 . Here, Ticket ID shows the ticket to be used from now on to 00005.

[0062] First, the authentication at the time of entrance is explained. Verification equipment 100 sends the information showing being entrance to certification equipment 200 with the authentication information C first (S32).

[0063] Certification equipment 200 generates the ticket judging information M. The contents of M are shown in drawing 10 . As shown in drawing, the contents included in ticket use information and the contents of entrance / participation record of an internal state to show a busy condition are included in the ticket judging information M. The certification information generation section 206 connects M with C, performs the signature by the ticket private key D, and sends it to verification equipment 100 with the 2nd generated authentication information chi as ticket certification information T (S34).

[0064] Verification equipment 100 verifies ticket certification information, and checks the contents of the ticket judging information M further. Here, since an entrance station is within an expiration date and is an intact ticket at the Yokohama station, it is judged with it being the ticket which may carry out authentication here (S35).

[0065] Then, the information mu for changing the internal state of certification equipment 200 is created. The contents of mu are shown in drawing 11 . An entrance name of the station and time amount are recorded on mu. The certification information generation section 103 connects with the 2nd authentication information chi mu generated in this way, generates the value rho which performed the signature using the privilege information delta on verification equipment 100, and sends it to certification equipment 200 (S36).

[0066] The value of rho to which the certification information verification section 205 of certification equipment 200 was sent checks whether it is in agreement with the authentication information chi. When it is able to be checked that it is a right thing, the internal-state control section 207 changes the internal state of certification equipment 200 according to the contents of mu (S37). The situation of the internal state after modification is shown in drawing 12 . It turns out that the station and time amount of entrance were recorded. Next, the internal-state control section 207 makes M' the contents of modification of this internal state, i.e., entrance record. Like an example 1, the certification information generation section 206 connects the value of M' with the bit string of authentication information, generates the value R which performed the signature by ticket confidential information, and sends it to verification equipment 100 as certification information R (S38).

[0067] When the value of the certification information R is verified and the value is in agreement with the authentication information C, verification equipment 100 checks M', as a result of changing an internal state further. If M' corresponds with what was specified by mu, it will be judged as that by which the internal state was changed correctly, and the gate of a ticket gate machine will be opened.

[0068] Next, the authentication at the time of participation is explained. Although the authentication at the time of participation is the same as that of the time of entrance almost, the contents of the message told mutually differ.

[0069] Verification equipment 100 sends the information showing being participation to certification equipment with the authentication information C first (S32).

[0070] The ticket judging information generation section 203 of certification equipment 200 generates the ticket judging information M. The contents of M at the time of participation are shown in drawing 13 . The certification information generation section 206 connects M with C, performs the signature by the ticket private key D, and is taken as the ticket certification information T. And the 2nd authentication information chi which carried out authentication information generation section generation with the certification information T is sent to verification equipment (S34).

[0071] The certification information verification section 104 of verification equipment 100 verifies ticket certification information. In a verification result [of a ticket], or right case, the ticket judging section 101 checks the contents of the ticket judging information M. Here, since an entrance station is effective entrance record and is within the shelf-life of participation at the Yokohama station, it is judged with it being the ticket which can attest participation here (S35).

[0072] Next, the certification information generation section 103 creates the information mu for changing the internal state of certification equipment 200. The contents of mu are shown in [drawing 14](#). A participation name of the station and participation time amount are recorded on mu. The certification information generation section 103 connects generated mu with chi further, and generates the value rho which performed the signature using the privilege information delta on verification equipment. rho is sent to certification equipment 200 (S36).

[0073] The value of rho to which the certification information verification section 205 of certification equipment 200 was sent checks whether it is in agreement with the authentication information chi. When the right thing is able to be checked, according to the contents of mu, the internal-state control section 207 changes the internal state of certification equipment 200, and makes it M' as a result of [this] modification (i.e., participation record). The situation of the internal state after modification is shown in [drawing 15](#). A participation station and time amount are recorded. The certification information generation section 206 connects participation record M' with the bit string of the authentication information C, generates the certification information R which performed the signature by ticket confidential information, and sends it to verification equipment 100 (S38).

[0074] When the value of R is verified and the value is in agreement with the authentication information C, the certification information verification section 104 of verification equipment 200 checks M', as a result of changing an internal state further. If M' corresponds with what was specified with the value of mu, it will be judged as that by which the internal state was changed correctly, participation will be permitted, and the gate of a ticket gate machine will be opened (S39).

[0075] The [example 3] example 3 shows how to realize a gestalt like a coupon ticket.

[0076] Fundamentally, the configuration of this example, the generation method of a ticket, and the flow of the whole processing are the same as that of an example 1. The configuration of whole this example is shown in [drawing 16](#). It differs in that counter 202a which shows the remaining frequency of a coupon ticket is installed in the internal state as a description of this example. In [drawing 16](#), the sign corresponding to [drawing 2](#) and a corresponding part was attached.

[0077] A user will register with certification equipment 200 first, if a coupon ticket is purchased. The internal-state storage region corresponding to a coupon ticket is secured at the time of registration, and the remaining use counts are written in counter 202a in it.

[0078] After a user specifies a coupon ticket with ticket assignment equipment 300 as a ticket used to certification equipment 200 after this, Challenge Handshake Authentication Protocol is started by the utilization time of a coupon ticket between verification equipment 100 and certification equipment 200.

[0079] At Challenge Handshake Authentication Protocol, it is the same as that of an example 1 till the place where verification equipment 100 generates a random number C as authentication information at, and delivery and certification equipment 200 calculate a ticket private key to certification equipment 200.

[0080] The flow chart of ticket certification information generation processing (it corresponds to S33 of [drawing 3](#)) of this example is shown in [drawing 17](#). In [drawing 17](#), the ticket judging information generation section 203 of certification equipment 200 extracts the count of the remainder of the internal state corresponding to the ticket of this coupon ticket, and records it on the ticket judging information M with ticket use information (S81-S84). And like an example 1, the certification information generation section 206 generates the ticket certification information T (S85), and the authentication information generation section 204 generates the 2nd authentication information chi (S86). T and chi are sent to verification equipment 100 by the communications department 208 (S34).

[0081] The verification equipment 100 which received T and chi performs ticket judging processing (it is ***** to S35 of [drawing 3](#)).

[0082] The flow chart of ticket judging processing is shown in [drawing 18](#). In [drawing 18](#), the certification information verification section 104 of verification equipment 100 verifies the received ticket certification information (S91). Ticket certification information extracts the ticket judging information M from ticket certification information to a right case (S92). The count of the remainder of a coupon ticket is recorded on the ticket judging information M. With [that value] one [or more], the

ticket judging section 101 judges that this coupon ticket is still usable (S93). Furthermore, when the ticket judging section 101 also judges [that it is verifiable with this verification equipment 100 and] the contents of the ticket use information L, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200 (S94, S95). The contents which direct to reduce the use count of a coupon ticket by one as contents of mu are included. And by the same approach as an example 1, the 2nd certification information rho is created using mu (S96, S97), and it sends to certification equipment 200 (S36).

[0083] Error processing is performed when verification and a ticket judging go wrong (S98).

[0084] The certification equipment 200 which received rho performs internal-state modification processing (it corresponds to S37 of drawing 3).

[0085] The flow chart of internal-state modification processing is shown in drawing 19 . In drawing 19 , the certification information verification section 205 of certification equipment 200 verifies the 2nd sent certification information rho (S101). When it is able to be checked that it is a right thing, according to the contents of mu, an internal-state control section reduces the remaining use count of a coupon ticket by one, and makes the result M' (S102-S104). The rest is the same approach as an example 1, and certification equipment 200 generates the certification information R, and sends it to verification equipment 100 (S105, S106). Error processing is performed when verification goes wrong at step S101 (S107).

[0086] Actuation of the subsequent verification equipments 100 is the same as that of an example 1, verifies the value of R and offers service.

[0087] In the example 4 of [example 4] this invention, although the whole configuration is the same as that of an example 1, the authentication approaches of ticket public information and ticket confidential information, or a ticket differ.

[0088] this example -- p -- the prime factor -- it is -- G -- dispersion -- a logarithm -- a finite group with a difficult problem -- it is -- g -- the origin of the order p of a finite group G -- it is -- [0089]

[Equation 14] $y = gx \bmod p$ When p is filled, (p, G, g, y) are ticket public information, and make x ticket confidential information. (p, G, g) can also be made common by the whole system.

[0090] At this time, a ticket is [0091] from the ticket description information x, the certification equipment proper information du, the ticket use information L, and the information p that specifies a group.

[Equation 15] $t = x - F(du, L, y, p)$

It is calculated by carrying out. Here, F is the one-way function of un-colliding nature, and a general Hash Function can realize it. L is the same ticket use information as an example 1.

[0092] Moreover, the above (p, G, g) is [0093] as common as a thing showing the privilege of verification equipment.

[Equation 16]

$$\eta = g^f \bmod p$$

***** -- let eta [like] into public information and let xi be confidential information.

[0094] G can be constituted as a multiplicative group in fact, or it can constitute as an elliptic curve on finite field.

[0095] The outline of the Challenge Handshake Authentication Protocol of this invention is shown in drawing 20 .

[0096] First, after a user specifies the ticket to be used from now on to certification equipment, Challenge Handshake Authentication Protocol is started between verification equipment and certification equipment.

[0097] In drawing 20 , by this Challenge Handshake Authentication Protocol, first, the authentication information generation section 102 of verification equipment 100 generates a random number r, calculates C=gr, and sends to certification equipment by making this into authentication information (S201, S202, S203).

[0098] The certification equipment 200 which received the authentication information C performs ticket

certification information generation processing (S204).

[0099] The flow chart of ticket certification information generation processing is shown in drawing 21. In drawing 21, the certification information generation section 206 of certification equipment 200 computes first the private key x used for a signature by the following count from p of Ticket t , the ticket use information L , and ticket public information, and the certification equipment proper information du (S211).

[0100]

[Equation 17]

$t+F(y,L,du,p)$

$=x-F(y,L,du,p)+F(y,L,du,p)$

= Generate the ticket judging information M to show that x , next the ticket judging information generation section 203 hold the right ticket from the additional information L of a ticket, and the information on an internal state (S212). The certification information generation section 206 generates the following values as certification information (S213, S214).

[0101]

[Equation 18] $T = (C||M)$ and $Cx \bmod p$ -- in addition, the certification information T is calculable with the following formulas besides the above.

[0102]

[Equation 19]

$T = (C||M)$ and $CtCF(y, L, du, p) \bmod p$ and the authentication information generation section 204 generate random-number r' to coincidence, and are [0103].

[Equation 20] $Chi = gr' \bmod p$ is sent to verification equipment as 2nd authentication information (S215, S216, S205). The information included in the ticket judging information M is the same as that of examples 1-3.

[0104] The certification information T and the 2nd authentication information chi are sent to verification equipment 100 by the communications department 208.

[0105] The verification equipment 100 which received T and chi performs ticket judging processing (S206 of drawing 20).

[0106] The flow chart of ticket judging processing is shown in drawing 22. It is [0107] from the ticket certification information that the certification information verification section 103 of verification equipment 100 was sent in drawing 22.

[Equation 21] $T/yr \bmod p = (C||M)$ and $Cx/yr \bmod p$ The value of p is calculated and it checks whether parts other than M connected among the bit string are in agreement with the authentication information C (S221). When in agreement, the ticket judging section 101 judges further whether it is what the internal state related with the ticket and the ticket may verify with this verification equipment 100 from the contents of the ticket judging information M (S222, S223). When this ticket may be verified as a result of a judgment, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200, and connects it with chi (S224, S225). And the following values are generated as 2nd authentication information to this value using the confidential information xi showing the privilege of verification equipment (S226).

[0108]

[Equation 22]

$\rho = (x || \mu) \cdot x^f \bmod p$

ρ is sent to certification equipment 200 by the communications department 106. On the other hand, when ticket certification information is not a right thing, or in being what a ticket should not verify, it ends a protocol (S227).

[0109] Next, the certification equipment 200 which received ρ performs internal-state modification processing (S208 of drawing 20).

[0110] The flow chart of internal-state modification processing is shown in drawing 23. It is [0111] from a response indication to which the certification information verification section 205 of certification

equipment 200 was sent in drawing 23 .

[Equation 23]

$$\rho / \eta^{t'} \bmod p = (x \parallel \mu) \cdot x^t / \eta^{t'} \bmod p$$

A ** value is calculated and it checks whether parts other than mu connected among the bit string are in agreement with the 2nd authentication information chi (S231). When it is able to be checked that it is a right thing, according to the information the internal-state control section 207 instructs modification of the internal state of mu to be, the internal state of certification equipment 200 changes and the result is made into M' (S232-S234). On the other hand, as a result of a check, when it becomes clear that it is not right, a protocol is ended to a case (S137).

[0112] after the certification information generation section 206 connects the value of M' with the bit string of the authentication information C -- the following values -- certification information -- ** -- it generates by carrying out (S235, S236).

[0113]

[Equation 24] $R = (C \parallel M')$ and $Cx \bmod p$ -- the certification information R generated in this way is sent to verification equipment 100 by the communications department 208 (S209).

[0114] The verification equipment 100 which received R performs certification information verification processing S210 (drawing 20).

[0115] The flow chart of certification information verification processing is shown in drawing 24 . It is [0116] from the ticket certification information that the certification information verification section 104 was sent in drawing 24 .

[Equation 25] $R/yr \bmod p$ The value of $p = (C \parallel M')$ and $Cx/yr \bmod p$ is calculated and, as a result, the bit string of the high order except M' checks that it is in agreement with the authentication information C which verification equipment 100 generated first (S241). The defined service is offered, when it checks whether the contents of information M' which expresses the modification result of an internal state further are in agreement with the information mu to which internal-state modification sent as 2nd certification information rho is permitted when it is able to check (S242, S243, S244) and a check is completed (S245). When one of checks goes wrong, a protocol is completed and offer of service is not performed (S246).

[Translation done.]

*** NOTICES ***

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a flow chart explaining processing of a related technique.

[Drawing 2] It is the block diagram showing the configuration of examples 1, 2, and 4 as a whole.

[Drawing 3] It is a flow chart explaining the whole processing of an example 1.

[Drawing 4] It is a flow chart explaining ticket certification information generation processing of the certification equipment of an example 1.

[Drawing 5] It is a flow chart explaining ticket judging processing of the verification equipment of an example 1.

[Drawing 6] It is a flow chart explaining internal-state modification processing of the certification equipment of an example 1.

[Drawing 7] It is a flow chart explaining certification information verification processing of the verification equipment of an example 1.

[Drawing 8] It is drawing showing the internal state in early stages of the token of an example 2.

[Drawing 9] It is drawing showing the item of ticket additional information.

[Drawing 10] It is drawing showing the ticket judging information M sent to a ticket gate machine from a token at the time of entrance.

[Drawing 11] It is drawing showing the item mu sent to a token from a ticket gate machine at the time of entrance.

[Drawing 12] It is drawing showing the internal state of the token after entrance.

[Drawing 13] It is drawing showing the ticket judging information M sent to a ticket gate machine from a token at the time of participation.

[Drawing 14] It is drawing showing the information mu sent to a token from a ticket gate machine at the time of participation.

[Drawing 15] It is drawing showing the internal state of the token after participation.

[Drawing 16] It is the block diagram showing the configuration of an example 3 as a whole.

[Drawing 17] It is a flow chart explaining ticket certification information generation processing of the certification equipment of an example 3.

[Drawing 18] It is a flow chart explaining ticket judging processing of the verification equipment of an example 3.

[Drawing 19] It is a flow chart explaining internal-state modification processing of the certification equipment of an example 3.

[Drawing 20] It is the flow chart which shows processing of an example 4 as a whole.

[Drawing 21] It is a flow chart explaining ticket certification information generation processing of the certification equipment of an example 4.

[Drawing 22] It is a flow chart explaining ticket judging processing of the verification equipment of an example 4.

[Drawing 23] It is a flow chart explaining an internal-state update process of the certification equipment of an example 4.

[Drawing 24] It is a flow chart explaining certification information verification processing of the verification equipment of an example 4.

[Description of Notations]

100 Verification Equipment
101 Ticket Judging Section
102 Authentication Information Generation Section
103 Certification Information Generation Section
104 Certification Information Verification Section
200 Certification Equipment
201 Certification Equipment Proper Information Attaching Part
202 Ticket Attaching Part
202a Counter
203 Ticket Judging Information Generation Section
204 Authentication Information Generation Section
205 Certification Information Verification Section
206 Certification Information Generation Section
207 Internal-State Control Section
300 Ticket Assignment Equipment

[Translation done.]

(19) 日本四特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出版公開番号

特開平11-225143

(43) 公開日 平成11年(1999) 8月17日

(51) Int. Cl.⁴

識別記号

F I

H 0 4 L 9/32

H 0 4 L 9/00

6 7 5 D

G 0 6 F 17/60

G 0 6 K 17/00

T

G 0 6 K 17/00

S

G 0 7 B 1/00

A

G 0 7 B 1/00

B

審査請求 未請求 請求項の数 41 O L (全 29 頁) 最終頁に続く

(21) 出願番号 特願平10-27074

(22) 出願日 平成10年(1998) 2月9日

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 水子 健一郎

神奈川県足柄上郡中井町430 グリーン

テクナール 富士ゼロックス株式会社内

(72) 発明者 中堀 寿平

神奈川県足柄上郡中井町430 グリーン

テクナール 富士ゼロックス株式会社内

(72) 発明者 京端 仁樹

神奈川県足柄上郡中井町430 グリーン

テクナール 富士ゼロックス株式会社内

(74) 代理人 弁理士 澤田 俊夫

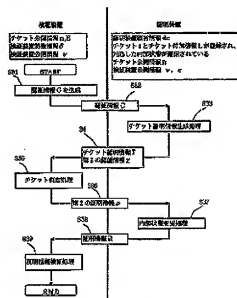
最終頁に続く

(54) 【発明の名称】 電子チケットシステム

(57) 【要約】

【課題】 誤って、または不正に提示されたチケットにより証明装置の内部状態が変更されないようにする。

【解決手段】 検証装置 100 の証明情報生成部 102 が、証明情報 C を生成し証明装置 200 に送る (S31、S32)。証明装置 200 のチケット判定情報生成部 203 は、正しいチケットを保持していることを示すためのチケット判定情報 M を、チケット利用情報および内部状態記憶領域の情報から生成する。証明情報生成部 206 は、証明情報 C のビット列の下位にチケット判定情報 M を連結し、チケット証明情報 T を生成する (S33)。チケット証明情報 T は、通信部 208 により検証装置 100 に送られる (S34)。T を受け取った検証装置 100 はチケット判定処理を行い、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないもの場合には、プロトコルを終了する (S35)。



実施例 1 の発明全体のフローチャート

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開

特開平11-

(43) 公開日 平成11年

(51) Int. Cl. ⁶	識別記号	P I	
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D
G 0 6 F 17/60		G 0 6 K 17/00	T
G 0 6 K 17/00			S
		G 0 7 B 1/00	A
G 0 7 B 1/00			B

審査請求 未請求 請求項の数41 O L (全 29 頁) J

(21) 出願番号 特願平10-27074

(22) 出願日 平成10年(1998) 2月9日

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 木子 健一郎

神奈川県足柄上郡中井町埴430

テクナカイ 富士ゼロックス

(72) 発明者 中垣 寿平

神奈川県足柄上郡中井町埴430

テクナカイ 富士ゼロックス

(72) 発明者 京嶋 仁樹

神奈川県足柄上郡中井町埴430

テクナカイ 富士ゼロックス

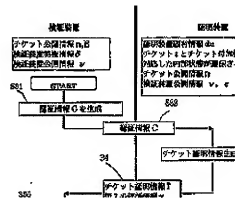
(74) 代理人 弁理士 澤田 俊夫

(54) 【発明の名称】 電子チケットシステム

(57) 【要約】

【課題】 誤って、または不正に提示されたチケットにより証明装置の内部状態が変更されないようにする。

【解決手段】 検証装置100の認証情報生成部102が、認証情報Cを生成し証明装置200に送る（S31、S32）。証明装置200のチケット判定情報生成部203は、正しいチケットを保持していることを示すためのチケット判定情報Mを、チケット利用情報および内部状態記憶領域の情報から生成する。証明情報生成部206は、認証情報Cのビット列の下位にチケット判定



(2)

待明平11-225143

1

【特許請求の範囲】

【請求項1】 証明装置と検証装置とを有し、上記証明装置が正当なチケットを所有していることを検証する電子チケットシステムであって、
上記証明装置は、

上記証明装置の固有情報を保持する証明装置固有情報保持手段と、

上記チケットを保持するチケット保持手段と、

上記チケットの権利内容または上記チケットの使用状態を表すチケット判定情報を生成するチケット判定情報生成部と、

少なくとも上記証明装置固有情報と上記チケットとからチケット秘密情報を生成し、上記チケット秘密情報を用いて証明情報を生成する証明情報生成手段とを有し、

上記検証装置は、

上記証明装置が提示する上記チケット判定情報に基づいて、検証処理を実行して良さを判定するチケット判定手段と、

上記証明装置がチケット秘密情報を生成できたか否かを、上記証明情報に基づいて、検証する証明情報検証手段とを有することを特徴とする電子チケットシステム。

【請求項2】 請求項1に記載の電子チケットシステムであって、

上記検証装置は、対話証明で用いられる認証情報を生成する認証情報生成手段を有し、

上記証明装置の証明情報生成手段は、上記検証装置が生成した認証情報を用いて上記証明情報を生成する電子チケットシステム。

【請求項3】 請求項2に記載の電子チケットシステムであって、上記証明装置と上記検証装置とは通信手段を有し、上記証明装置は証明しようとするチケットのチケット判定情報を、上記検証装置に伝送する電子チケットシステム。

【請求項4】 請求項2ないし3に記載の電子チケットシステムであって、
上記電子チケットシステムは、上記検証装置と上記証明装置とに加えて、チケット発行装置を有し、
上記チケット発行装置は、

発行するチケットの秘密の特徴情報である上記チケット秘密情報と対応するチケット公開情報を保持するチケット特徴情報保持手段と、

利用者が保持する上記証明装置の固有情報を保持するチケット発行用証明装置固有情報保持手段と、

上記チケット特徴情報保持手段に保持している上記チケット秘密情報と、上記チケット発行用証明装置固有情報保持手段に保持している上記証明装置固有情報とを用いて、

デジタル情報であるチケットを作成するチケット発行手段を有する電子チケットシステム。

【請求項5】 請求項2ないし4の電子チケットシステムであって、上記証明装置の証明情報生成手段は、少な

2

くとも上記検証装置から送られた認証情報と、上記チケットと、上記チケット判定情報と、上記証明装置固有情報とより所定の方法で、上記証明情報の1つとして、上記チケット判定手段の判定に用いるチケット証明情報を計算する電子チケットシステム。

【請求項6】 請求項5に記載の電子チケットシステムであって、上記証明装置はチケットの利用条件を定めたチケット利用情報を、チケットと対応させて上記チケット保持部に保持する電子チケットシステム。

【請求項7】 請求項5に記載の電子チケットシステムであって、上記証明装置は、上記チケット判定情報を作成する際に、少なくとも上記チケット利用情報を用いる電子チケットシステム。

【請求項8】 請求項6に記載の電子チケットシステムであって、上記証明装置は、可変な内部状態を保持する内部状態記憶領域と、上記内部状態の値を制御する内部状態制御手段とを備える電子チケットシステム。

【請求項9】 請求項8に記載の電子チケットシステムであって、上記証明装置のチケット判定情報生成手段は、上記チケット判定情報を作成する際に、少なくとも上記証明装置の内部状態記憶領域の情報をを用いる電子チケットシステム。

【請求項10】 請求項8ないし9の電子チケットシステムであって、上記証明装置の内部状態記憶領域が保持する可変な内部状態のうちの、少なくとも一部は外部から書き換え不能である電子チケットシステム。

【請求項11】 請求項8ないし10の電子チケットシステムであって、上記証明装置の証明情報生成手段は、少なくとも、上記チケットと、上記チケット利用情報と、上記証明装置固有情報とを用いて上記証明情報を計算する電子チケットシステム。

【請求項12】 請求項8ないし11の電子チケットシステムであって、上記証明装置は、上記検証手段から送られた上記認証情報を保持する認証情報保持手段を有し、上記証明情報生成手段は、上記チケット判定情報生成手段により生成されたチケット判定情報を用いて、上記認証情報保持手段に保持されている認証情報を変更して上記証明情報の生成に利用する電子チケットシステム。

【請求項13】 請求項12の電子チケットシステムであって、上記チケット判定情報生成手段が生成したチケット判定情報をMとし、上記認証情報をCとすると、上記証明装置の証明情報生成手段は、上記認証情報保持手段に保持されている認証情報Cを、CにMを複合したものに更新する電子チケットシステム。

【請求項14】 請求項12ないし13の電子チケットシステムであって、上記証明装置の証明情報生成手段は、上記証明情報の1つとしてチケット証明情報を生成することが可能であり、上記チケット証明情報、上記チケットと、上記チケット利用情報と、上記証明装置固有

(3)

特開平11-226143

有情報とより所定の方法でチケット秘密情報を計算し、上記認証情報に対して、チケット秘密情報を用いた計算

【請求項15】 請求項14の電子チケットシステムであって、 p, q が素数であり、 $n = p \cdot q$ であり、 $DE \equiv 1 \pmod{(p-1)(q-1)}$ の関係が満たされるとき、上記チケット秘密情報が D であり、チケット公開情報が (n, E) であり、上記チケット利用情報が L であり、上記証明秘密鍵固有情報が秘密の値 d であり、 $f(d, u, L, n)$ を一方方向性関数として、チケットが
 $t = D - f(d, u, L, n)$ で与えられているとき、上記証明秘密鍵の証明情報生成手段は、上記認証情報 C （上記証明情報生成手段が変更した認証情報）に対して、 C の法 n での1による乗算と、 C の法 n での一方方向性関数値 $f(d, u, L, n)$ による乗算との法 n での積 $C' \equiv C \cdot f(d, u, L, n) \pmod{n}$ としてチケット証明情報を計算する電子チケットシステム。

【請求項16】 請求項14の電子チケットシステムであって、 p, q が素数であり、 $n = p \cdot q$ であり、 $DE \equiv 1 \pmod{(p-1)(q-1)}$ の関係が満たされるとき、上記チケット秘密情報が D であり、チケット公開情報が (n, E) であり、上記チケット利用情報が L であり、上記証明秘密鍵固有情報が秘密の値 d であり、 $f(d, u, L, n)$ を一方方向性関数として、上記チケットが
 $t = D - f(d, u, L, n)$ で与えられているとき、上記証明鍵は、あらかじめ $t + f(d, u, L, n) = D$ を計算し、その値を用いて、上記認証情報 C （上記証明情報生成手段が変更した認証情報）に対して、 $T = C' \pmod{n}$ としてチケット証明情報 T を計算する電子チケットシステム。

【請求項17】 請求項14の電子チケットシステムであって、 g が楕円曲線問題が困難な群の原始根であり、 p が素数であり、整数 x に対して $y = g^x \pmod{p}$ が成り立つとき、上記チケット秘密情報が x であり、チケット公開情報が (y, p, g) であり、上記チケット利用情報が L であり、上記証明秘密鍵固有情報が秘密の値 d であり、 $f(d, u, L, y)$ を一方方向性関数として、上記チケットが
 $t = x - f(d, u, L, y)$ で与えられているとき、上記証明鍵は、上記認証情報 C （上記証明情報生成手段が変更した認証情報）に対して、上記チケット判定情報 T を C の法 p での1による乗算と、 C の法 p での一方方向性関数値 $f(d, u, L, y)$ を指数とする乗算との法 p での積 $C' \equiv C^{f(d, u, L, y)} \pmod{p}$ として上記証明情報を計算する電子チケットシステム。

【請求項18】 請求項14の電子チケットシステムであって、 g が楕円曲線問題が困難な群の原始根であり、 p が素数であり、整数 x に対して $y = g^x \pmod{p}$ が成り立つとき、上記チケット秘密情報が x であり、チケット公開情報が (y, p, g) であり、上記チケット利用情報が L であり、上記証明秘密鍵固有情報が秘密の値 d

u であり、 $f(d, u, L, y)$ を一方方向性関数として、上記チケットが
 $t = x - f(d, u, L, y)$ で与えられているとき、上記証明鍵は、あらかじめ $t + f(d, u, L, y) = x$ を計算し、上記認証情報 C に対して（上記証明情報生成手段が変更した認証情報）チケット判定情報 T を計算する際に、 $C' \pmod{p}$ の値を用いる電子チケットシステム。

【請求項19】 請求項14ないし18の電子チケットシステムであって、上記検証秘密鍵の証明情報検取手段は、上記証明情報生成手段が作成した認証情報と、上記証明秘密鍵から送られたチケット証明情報と、上記チケット公開情報とより、上記チケット証明情報の正当性を検証し、上記チケット証明情報が正しい場合は、上記チケット証明情報に収められたチケット判定情報を導出する電子チケットシステム。

【請求項20】 請求項19の電子チケットシステムであって、上記認証情報が C であり、上記チケット証明情報が T であり、上記チケット公開情報が (n, E) であり、あるビット列 M がある場合に、上記検証秘密鍵の証明情報検取手段は、上記チケット証明情報 T を法 n で E でべき乗したものを C と M とを結合したビット列と比較し、 $T^E \pmod{n} = C \parallel M$ （記号 \parallel はビット列の結合）となっていれば、上記チケット証明情報は正しいと判定し、上記チケット証明情報が正しい場合は M を上記チケット判定情報として導出する電子チケットシステム。

【請求項21】 請求項19の電子チケットシステムであって、上記認証情報が C であり、上記チケット証明情報が T であり、上記チケット公開情報が (p, g, y) である場合に、上記検証秘密鍵の証明情報検取手段は、自身が発生させた乱数 r とすると、あるビット列 M があり、 $T/y^r \pmod{p} = C \parallel M$ （記号 \parallel はビット列の結合）となっていれば、上記チケット証明情報は正しいと判定し、上記チケット証明情報が正しい場合は M をチケット判定情報として導出する電子チケットシステム。

【請求項22】 請求項8ないし21の電子チケットシステムであって、

上記証明鍵は、上記検証秘密鍵を認証するための第2の認証情報を生成する、第2の証明情報生成手段と、上記検証秘密鍵が生成する第2の証明情報を検定するための、第2の証明情報検取手段とを有し、
 上記第2の証明情報検取手段は、上記第2の認証情報と、上記第2の証明情報と、チケット公開情報とより上記第2の証明情報が正しいかどうかを検定し、
 上記第2の証明情報が正しい場合、上記内部状態制御手段は、上記証明秘密鍵の内部状態を変更する電子チケットシステム。

【請求項23】 請求項22の電子チケットシステムであって、上記検証秘密鍵の証明情報検取手段は、上記チケ

(4)

特開平 11-226143

5

ット判定手段による判定の結果をもとにして、上記第2の証明情報を生成するか否かを決定する電子チケットシステム。

【請求項24】 請求項22の電子チケットシステムであって、

上記証明装置は、チケットのカウンタとして機能する内部状態をチケットに関連づけ、外部から書き換え不能な形で、内部状態記憶領域に保持し、

上記検証装置の証明情報検証手段は、上記証明装置から送られたチケット判定情報に含まれる内部状態のカウンタの値が、所定の値であるときには、対応するチケットが無効であるものと判断する電子チケットシステム。

【請求項25】 請求項22ないし24の電子チケットシステムであって、 p^* 、 q^* が素数であり、 $v = p^* \cdot q^*$ であり、 $e \equiv 1 \bmod (p^* - 1) \cdot (q^* - 1)$ の関係が満たされるときに、上記証明装置の第2の証明情報検証手段は、上記第2の認証情報と上記第2の証明情報 ρ が

【数1】

$$x = \rho^e \bmod v$$

を満たす場合に上記第2の証明情報が正しいと判定する電子チケットシステム。

【請求項26】 請求項22ないし24の電子チケットシステムであって、 g が素数対数範囲で固な群の原始元

$$x \mid \mid \mu = \rho^e \bmod v$$

を満たすときに、上記第2の証明情報が正しいと判定し、 μ を上記第2の証明情報に埋め込まれた情報として導出する電子チケットシステム。

【請求項30】 請求項27の電子チケットシステムであって、上記証明装置の内部状態制御手段は、上記第2の証明情報から導出された情報にもといて、上記内部状態記憶領域に保持された内部状態を変更する電子チケットシステム。

【請求項31】 請求項30の電子チケットシステムであって、上記証明装置の上記第2の証明情報検証手段は、上記検証装置より送られた内部状態変更を許可する情報と、内部状態に基づいて、上記証明情報を正しく生成するか否かを判定する電子チケットシステム。

【請求項32】 請求項22ないし31の電子チケットシステムであって、上記検証装置は、上記検証装置の特徴を表す秘密情報である、検証装置特徴情報を保持する検証装置特徴情報保持部と、上記第2の証明情報を生成する第2の証明情報生成部を有し、

上記第2の証明情報生成部は、上記第2の認証情報と上記検証装置特徴情報とより第2の証明情報を生成する電子チケットシステム。

【請求項33】 請求項32の電子チケットシステムであって、上記検証装置特徴情報を δ とし、対応する公開情報を (v, e) とすると、上記検証装置の第2の証明情報生成部は、上記第2の認証情報 x より上記第2の

6

*根であり、 p が素数であり、 δ が素数に対して

【数2】

$$\eta = g^e \bmod p$$

が成り立つときに、証明装置の第2の認証情報生成手段は、乱数 r^* と上記第2の認証情報 $x = g^r$ を生成し、上記第2の証明情報検証手段は上記第2の証明情報 ρ について、 $\rho / \eta^{r^*} \bmod p = x$ が満たされた場合に上記第2の証明情報が正しいと判定する電子チケットシステム。

【請求項27】 請求項22の電子チケットシステムであって、上記証明装置の第2の証明情報検証手段は、上記第2の証明情報が正しい場合は、上記第2の証明情報に埋め込まれた情報を導出する電子チケットシステム。

【請求項28】 請求項27の電子チケットシステムであって、上記証明装置の第2の証明情報検証手段は、上記第2の証明情報から導出された情報を、上記内部情報の変更を許可するための情報として利用する電子チケットシステム。

【請求項29】 請求項27ないし28の電子チケットシステムであって、チケット公開情報は δ および e を含んでおり、上記証明装置の第2の証明情報検証手段は、上記第2の認証情報 x と上記第2の証明情報 ρ とが、あるビット列 μ に対して、

【数3】

(記号 $\mid \mid$ はビット列の接合)

証明情報 ρ を

【数4】

$$\rho = x^e \bmod v$$

として生成する電子チケットシステム。

【請求項34】 請求項32の電子チケットシステムであって、上記検証装置特徴情報を δ 、対応する公開情報を (p, g, n) とし、

【数5】

$$\eta = g^e \bmod p$$

の関係が満たされるとき、上記検証装置の第2の証明情報生成部は上記第2の認証情報 x に対して、

【数6】

$$x^e \bmod p$$

の値を用いて上記第2の証明情報 ρ を生成する電子チケットシステム。

【請求項35】 請求項32ないし34の電子チケットシステムであって、上記検証装置は上記第2の認証装置を保持する、第2の認証情報保持部を有し、上記検証装置の第2の証明情報生成部は、上記検証装置特徴情報を用いた計算を施す際に、証明装置の内部状態の変更を許可する情報と、上記第2の認証情報より上記第2の証明情報を計算する電子チケットシステム。

【請求項36】 請求項32ないし34の電子チケットシステムであって、上記検証装置の第2の証明情報生成部は、上記検証装置特徴情報を用いた計算を施す前に、

7

上記証明装置の内部状態の変更を許可する情報を用いて、上記第2の認証情報保持部に保持された上記第2の認証情報を更新する電子チケットシステム。

【請求項37】 請求項36の電子チケットシステムであって、上記検証装置の第2の証明情報生成部は、上記証明装置の内部状態の変更を許可する情報を μ とし、上記第2の認証情報を κ とすると、上記第2の認証情報保持部に保持された第2の認証情報を κ に μ を複合したものに更新する電子チケットシステム。

【請求項38】 請求項1ないし37に記載の電子チケットシステムであって、少なくとも、上記証明装置が、内部のデータ及び処理手続きを外部から観測することを困難ならしめる防衛手段中に保持されている電子チケットシステム。

【請求項39】 請求項1ないし37に記載の電子チケットシステムであって、少なくとも、上記証明装置が、ICカードなどの携帯可能な小型演算装置として構成されている電子チケットシステム。

【請求項40】 証明装置と検証装置とを有し、上記証明装置が正当なチケットを所有していることを検証する電子チケットシステムであって、

上記証明装置は、
上記証明装置の固有情報を保持する証明装置固有情報保持手段と、

上記チケットを保持するチケット保持手段と、
上記チケットの権利内容または上記チケットの使用状態を表すチケット判定情報を生成するチケット判定情報生成部と、

少なくとも上記証明装置固有情報と上記チケットとから証明情報を生成する証明情報生成手段とを有し、

上記検証装置は、

上記証明装置が提示する上記チケット判定情報に基づいて、検証処理を実行して良いかを判定するチケット判定手段と、

上記証明装置が上記証明装置固有情報と上記チケットから上記証明情報を生成してきた否かを検証する証明情報検証手段とを有することを特徴とする電子チケットシステム。

【請求項41】 検証装置と電子チケットを保持する認証装置との間で相互認証を行ないながら検証装置側で

(5)

特開平11-

8

【発明の属する技術分野】本発明は、チケットを電子的に作成し利用する技術に関する、【0002】

【背景の技術】【従来の技術】近年、乗指定券、予約券、回数券、定期券、ポイントカード、などの一般的なチケットとして発行する試みが行われている、【0003】このような電子チケットは、

ユーザーに与えた権利を特定でき、正しいことを検証できるという機能を持つ。電子容易であり、通信回線を通して送達でき、持つが、完全なコピーを簡単に作れるのトの実現には、偽造と複製による不正利用可欠である。電子署名により偽造の防止製の防止は困難であり、複製による不正ことが、電子チケットの実現にあたってなっていた。

【0004】この問題に対する、解決策チケットの利用時に正当な利用者が確認技術、発行者以外の者が勝手にチケットを複写ない第2の従来技術、検証時の通信を公第2の従来技術を修正した第3の従来技法が提案されてきた。

【0005】第1の従来技術は、チケットユーザーが、正当な利用者かどうかを確認する。利用者は、チケットを利用する時に、特に、自分が利用者特定情報に適合する正しることを示す。利用者特定情報に適合しする権利の行使が認められる。確認のため（利用者特定情報）と、与えた権利とを：がチケットとして発行され、利用者が発行者以外の者が勝手にチケットを偽造するためには、発行者がチケットに電子署名のないチケットは、偽造されたもの利用者特定情報には、身元、顔写真などパスワードなどの知識の所有などが利用【0006】しかしながら、この方法で利用者特定情報に応じて、いくつかの問題【0007】例えば、利用者特定情報に：利用する方法では、発行時と検証時に利

40

(5)

特開平11-225143

9

19

【0009】第2の従来技術は、例えば特開平8-147500号公報に示されるようなものであり、発行者以外の者にチケットを復写する機会を与えない方法である。この方法では、利用者が保持管理しているチケットを復写できないようにする機構と、発行時や検証時の通信からチケットが漏洩しない機構の両方を必要とする。

【0010】しかしながら、この方法では

(1) 発行者以外の者はチケットを復写できないので、チケットの正当性を第三者に証明することが困難になる。(2) チケットの発行時と検証時の通信の内容も機密に行うので、チケットの発行時と検証時にプライバシーなどの利用者の権利が侵害されていないことを証明できない、といった問題が生ずる。

【0011】第3の従来技術は、例えば特開平6-52518号公報に示されるようなものであり、検証時の通信を公開できるように、第2の従来技術を修正した方法である。この方法では、第2の従来技術と同様に、チケットを秘密情報として利用者の所持する装置(証明装置)に復写できないように記録するが、検証の方法が異なる。まず、検証を行う検証装置は、証明装置に乱数などの値を送り利用されない値(チャレンジ)を送る。証明装置は、チャレンジである秘密情報を利用した演算をチャレンジに対して施して、得られた値(レスポンス)を検証装置に送り返す。検証装置は、秘密情報とチャレンジを利用してレスポンスが演算されたことを確認することで、利用者の正当性を認証する。レスポンスから逆に秘密情報を求めることを計算量的に困難とすることで、チャレンジとレスポンスを秘密通信とする必要がなくなる。

【0012】この方法は、認証のために利用されるものであり、正当なチケットを保持しているか否か以外に情報を伝達しない。このため、有効期限などを示すことができず、単純なチケットしか実現できない。また、チケットを証明装置に送信する方法が、第2の従来技術と同様に秘密通信で行う必要があり、不当に利用者の情報を開示して利用者の権利を侵害していないことを証明できないという問題があった。

【0013】このように、従来の技術はいずれも、チケットに必要な不正利用を防止する機能を実現するために、第三者に対するチケットの内容証明の機能や利用者の匿名性を犠牲にしている点に、問題があった。

【0014】[関連技術] これらの問題を解決する関連技術として、特開平9-188064号(平成9年7月14日、未公開)に示す方法が知られている。

【0015】この関連技術の一般的な認証プロトコルを図1に示す。このプロトコルは、双方向の認証を行うプロトコルであり、双方が認証情報(発生した乱数)に対する署名を認証することによって、お互いの正当性を認証する。相互の認証情報(乱数)の一部にメッセージ(m, μ)を含ませることにより、情報の安全な伝達を

可能にしている。

【0016】図1を参照して関連技術のプロトコルについて説明する。図1において、はじめに、検証装置が乱数に基いて認証情報Cを生成し(S11)、この認証情報Cを証明装置に送り送る(S12)。他方、証明装置は乱数に基いて別の認証情報xを生成し、認証情報xを検証装置に送る(S13、S14)。証明装置にはチケットに対応して、外部からは操作不能な内部状態があり、検証装置からの応答情報によってのみ書き換えが可能となっている。検証装置はxの一部に、内部状態の変更を許可する情報(μ)を含ませた応答情報を作成し、検証装置に署名して証明装置に送る(S15、S16)。証明装置は応答情報μの署名を認証することにより、送信者が正当な検証装置であることを確認し、それをもって内部状態変更の情報μの正しさを確認する(S17)。μが正しい場合にのみ、証明装置の内部状態がμの内容にしたがって変更される(S18)。証明装置は、正当に作成されたチケットと証明装置固有情報dμから、Dを復元することが可能であり(S19)、最後に証明情報RにDによる署名を施して、検証装置に送り(S20、S21)、検証装置はその署名を認証することにより、定められたサービスを提供する(S22、S23)。

【0017】この方法によれば、チケットの検証情報は公開であるため第三者にもチケットの検証が可能であり、利用者はチケットの検証時に利用者を特定する情報を提示する必要が無いことから、匿名性が守られている。

【0018】また、検証装置と証明装置がそれぞれの秘密情報と公開情報を持ち合い、相互の認証をすることにより、証明装置・検証装置の偽造の問題を解決している。さらに、この証明に用いる認証情報の一部に、伝達したい情報を埋め込むことにより、検証装置・証明装置相互の情報伝達を可能にしており、チケットの内容を証明することができる。

【0019】このように、この関連技術の方法を使うと、電子チケットの基本的な機能をすべて満たした安全な電子チケットを実現することができ、上記の問題をすべて解決することが可能である。

【0020】ところで、先の関連技術では、検証装置がチケットを特定する情報を証明装置に送ることにより、検証装置が検証しようとするチケットが証明装置の中で一意に定まることを前提としている。しかし、実際には、その検証装置で検証可能なチケットが証明装置内に複数存在することも考えられる。たとえば、紙造の乗車券のようなものを考えた場合、その駅から有効な回数券や定期券など複数のチケットが証明装置の中に存在することがありう。そのような場合、証明装置では、どのチケットを利用者が利用しようとしているのか判断することができない。そこで、こういった場合には、利用者

11

があらかじめ利用するチケットを選択する必要が生ずる。

【0021】そして、このような場面において、先の関連技術を適用すると、チケットに対応する内部状態の変更を許可する応答情報か、選択・提示されたチケットの内容を確認することなしに作成され、送られてしまうという問題が生ずる。

【0022】これは、例えば、利用者が誤ったチケットを選択してしまった場合に、意図しないチケットの内部状態が変更されてしまうことを意味している。

【0023】また、鉄道の入場切符に適用する場合を考えると、内部状態として、入場の記録を残しておく、出場時に入場の記録を確認することにより、キセルのような不正行為を防止することが考えられる。

【0024】ここで、入場の情報として、単に入場したという事実のみを、チケットに対応する内部状態に残すような場合を考える。このような場合、内部状態の変更許可情報、具体的には入場情報を、提示されたチケットの内容を確認することなく、証明装置に送ってしまうと、本来その駅では入場できないチケットに対しても、入場

したという事実を残すことが可能になる。実際には正当でないチケットでの入場はできないが、入場を拒否されている段階で、内部状態を書き換えられたチケットを保持している証明装置を手に入れたことができるとすると、実際に入場した駅よりも目的駅に近い駅からのチケットに対する入場記録を偽造すれば、出場時に偽造した入場記録を持つチケットを提示することで、キセル行為が可能になってしまう。

【0025】このように、利用者が、証明しようとするチケットを自ら選択するような場合には、検証装置は、内部状態を変更する許可情報を作成する前に、提示されたチケットがその検証装置で正当に検証可能であることを確認する必要がある。

【0026】しかし、先の関連技術においては、このような検証が成されないため、利用者が誤って意図しないチケットに対応する内部状態を書き換えてしまったり、内部状態を書き換えることによる不正が可能であったりするという問題点があった。

【0027】

【発明が解決しようとする課題】本発明では、上記の問題を解決するために、検証装置が検証可能なチケットのみを検証し、検証することが正しいチケットに対しては、内部状態の変更を許可する情報を生成しないような電子チケットシステムを実現することを目的とする。

【0028】

【課題を解決するための手段】上記の課題を解決するため、本発明に係る電子チケットシステムは、チケット検証装置と証明装置からなり、チケット検証装置は、検証するチケットが検証装置で検証可能かどうかを、証明装置が提示するチケット判定情報に基づいて判定するチ

(7)

特開平11-225143

12

ケット判定手段と、証明装置がチケット秘密情報を算出できたかどうかを検証する対話検証手段を有し、証明装置は、証明装置固有情報保持手段と、チケット保持手段と、少なくとも証明装置固有情報とチケットからチケット秘密情報に関する知識の証明を行える対話証明手段とを有している。

【0029】この構成においては、検証装置が、チケット判定情報に基づいて、証明装置内のチケットの適合性をチェックでき、正しいチケットが提示されたときのみ証明装置の内部状態を変更するようにできる。

【0030】

【発明の実施の態様】以下、本発明を詳細に説明する。

【0031】【実施例1】図2に本発明の実施例1の電子チケットシステムの構成図を示す。図2において、本実施例に示す電子チケットシステムは、検証装置（検証器ともいう）100と証明装置（証明器ともいう）200とチケット判定装置300とからなる。

【0032】検証装置100は、検証するチケットの正当性を判定するチケット判定部101と、認証情報生成部102と、証明情報生成部103と、証明情報検証部104と、検証装置特権情報保持部105と、通信部106とをきんで構成される。

【0033】一方、証明装置200は、証明装置固有情報保持部201と、チケット保持部202と、チケット判定情報生成部203と、認証情報生成部204と、証明情報検証部205と、証明情報生成部206と、内部状態制御部207と、通信部208とをきんで構成される。なお検証装置100の証明情報生成部103、認証装置200の証明情報生成部206は、それぞれ認証装置200、検証装置100から送られてくる認証情報を保持する記憶部を具備している。

【0034】また、チケット保持部202にはチケットと、各チケットに対応するチケット利用情報とが保管される。また、チケット保持部202には各チケットに対応する内部状態記憶領域が確保される。

【0035】ここでは、証明装置200は、内部のデータや処理手続きを外部から隠蔽することが困難なICカードのような媒体により構成される。

【0036】また、この実施例では以下のように、チケットが発行される。

【0037】

【表1】

チケット： $t = D - F \langle n, L, du \rangle$

D：チケット秘密鍵

du：証明装置固有の秘密情報

n：チケット注数

F：非回文性一方向関数

L：チケット利用情報

ただし、

$ED \equiv 1 \pmod{n}$

(8)

特開平11-226143

13

ここでE:チケット公開鍵である。チケット秘密情報はDであり、チケット公開情報は、E、n、Lである。Fは一般のハッシュ関数によって実現可能である。また、チケット利用情報には、そのチケットを利用する条件、例えば有効期限や、サービスを受けられる場所などの情報が入る。

【0038】本発明の認証プロトコルの概略を図3に示す。はじめに利用者は、これから利用するチケットをチケット指定装置300により証明装置200に指定した上で、検証装置100と証明装置200との間で認証プロトコルが開始される。

【0039】図3において、認証プロトコルでは、まず検証装置100の認証情報生成部102が、認証情報として乱数Cを生成し証明装置200に送る(S31、S32)。

【0040】認証情報を受け取った証明装置200は、チケット証明情報生成部206は、署名に用いる秘密鍵Dを、チケットIとチケット利用情報および証明装置固有情報保持部201に保存されている証明装置固有情報duから、以下の計算により算出する(S41)。

【0042】
【数7】
$$t + F(n, L, du)$$

$$= D - F(n, L, du) + F(n, L, du)$$

$$= D$$

次に、チケット判定情報生成部203は、正しいチケットを保持していることを示すためのチケット判定情報Mを、チケット保持部202のチケット利用情報および内部状態記憶領域の情報から生成する(S42)。証明情報生成部206は、認証情報Cのビット列の下位にチケット判定情報Mを連結し(S43)、チケット証明情報Tを、

【0043】
【数8】
$$T = (C || M)^s \bmod n$$

の計算により生成する(S44、なお記号||はビット列に連結することを示す)。なお上記の計算以外にも、

【0044】
【数9】
$$T = (C || M)^t (C || M)^{t(n-1, n-2)} \bmod n$$

により、証明情報Tを計算しても良い。

【0045】また、認証情報生成部204は、乱数xを生成し第2の認証情報とする(S44)。

【0046】チケット証明情報Tと第2の認証情報xは、通信部208により検証装置100に送られる(S4)。署名をするのは、チケット証明情報が正しいものであり、証明装置・チケット判定情報が偽造されていないことを保証するためである。

14

【0047】Tとxを受け取った検証装置100はチケット判定処理(図3のS35)を行う。

【0048】チケット判定処理(図3のS35)のフローチャートを図5に示す。図5において、検証装置100の証明情報検証部104は、送られたチケット証明情報Tと証明情報検証部が保持しているチケット公開情報Eから、

【0049】
【数10】
$$T^t \bmod n$$

の値を計算し、そのビット列のうち、連結された上位ビットの部分が、認証情報Cと一致するかどうかを認証する(S51)。一致した場合には、さらにチケット判定情報Mを抽出する(S52)。次に、チケット判定部101は、Mの内容をもとにチケット及びチケットに関連付けられた内部状態がこの検証装置で検証して良いものかどうかを判定する(S53)。判定の結果、このチケットを検証して良い場合には、証明情報生成部103は、証明装置200の内部状態の変更を指示する情報uを作成して、xの下位に連結する(S54、S55)。さらに、この値に対して、検証装置の特徴を表す秘密情報sを用いて署名をした値vを作成する(S56)。作成されたvは、通信部106により証明装置200へと送られる(S36)。

【0050】一方、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないもの場合には、プロトコルを終了する(S57)。

【0051】次にuを受け取った証明装置は内部状態変更処理(図3のS37)を行う。

【0052】内部状態変更処理(図3のS37)のフローチャートを図6に示す。図6において、証明装置200の証明情報検証部205は、送られた第2の証明情報xに対して、自身が保持している検証装置100の特徴を認証する公開情報sを用いて

【0053】
【数11】
$$\rho^s \bmod v$$

を計算し、そのビット列のうち、上位の部分が、第2の認証情報xと一致するかどうかを認証する(S61)。認証の結果、正しいことが判明した場合には場合には、プロトコルを終了する(S62)。正しいものであることが確認できた場合には、連結されたuを抽出する(S63)。内部状態制御部207は、uの内容に応じて証明装置200の内部状態を変更し、その結果をM'とする(S64、S65)。証明情報生成部206はM'の値を認証情報Cのビット列に連結した上で、

【0054】
【数12】
$$R = (C || M')^s \bmod n$$

の計算により、証明情報Rを生成する(S66、S67)。Rは通信部208により検証装置100に送られる(S38)。

(9)

待間平11-225143

15

【0055】Rを受け取った検証装置100は、証明情報検証処理（図3のS39）を行う。

【0056】証明情報検証処理（図3のS39）のフローチャートを図7に示す。図7において、検証装置100の証明情報検証部104は保持しているチケット公開情報を用いて、

【0057】

【数13】 $R^d \bmod n$

の値を計算し、その結果直結されたM'を除いた上位のビット列が、最初に検証装置100が生成した認証情報Cと一致することを確認する（S71）。確認できた場合は、さらに内部状態の変更結果を表す情報M'の内容が、第2の証明情報ρとして送った。内部状態変更を許可する情報μと一致するかどうかを確認し（S72、S73、S74）、確認できた場合には、定められたサービスを提供する（S75）。いずれかの確認に失敗した場合には、プロトコルが終了し、サービスの提供は行われない（S71、S74、S76）。

【0058】【実施例2】本発明の実施例2は、実施例1を旅客の切符の乗車券として実現した場合である。こ

こでは特に、乗車券の入場時のプロトコルを説明する。【0059】本発明の実施例の構成やチケットの生成方法は実施例1と同様であるが、検証装置100は具体的には自動改札機であり、証明装置200はチケットを保持することができ、ICカードのようなトークンである。そして、入場、出場ともに自動改札による検証が行われ、内部状態は入場や出場に対応した記憶領域が確保されるものとする。

【0060】以下では、横浜～成田空港1997年7月18日の乗車券の例で説明する。なお、追加、図3の対応するステップ等を指摘する。

【0061】チケットのチケット利用情報Lは、図9のようになる。チケットは証明装置200に登録されており、対応した内部状態記憶領域が確保されている。入場時の内部状態を図8に示す。ここで、これから使用するチケットは、チケットIDが00005に示すものである。

【0062】まず、入場時の認証について説明する。はじめに検証装置100は認証情報Cとともに、入場であることをあらわす情報を証明装置200に送る（S32）。

【0063】証明装置200は、チケット判定情報Mを生成する。Mの内容を図10に示す。チケット判定情報Mには、図に示すように、チケット利用情報に含まれる内容と、使用状態を示すための、内部状態の入場・出場記録の内容が含まれている。証明情報生成部206は、MをCに連結し、チケット秘密鍵Dによる署名を施して、チケット証明情報Tとして、生成した第2の認証情報ρとともに検証装置100に送る（S34）。

【0064】検証装置100は、チケット証明情報を検

16

証し、さらにチケット判定情報Mの内容を確認する。ここでは、入場駅が横浜駅で、有効期限内であり、未使用のチケットであることから、ここでの認証をよいチケットであると判定される（S35）。

【0065】そこで、証明装置200の内部状態を変更するための情報μが作成される。μの内容を図11に示す。μには、入場駅名と時間が記録される。証明情報生成部103は、こうして生成したμを第2の認証情報ρに連結し、検証装置100の検証情報ρによる署名を施した値ρを生成して、証明装置200へ送る（S36）。

【0066】証明装置200の証明情報検証部205は、送られたρの値が、認証情報ρと一致するかどうかを確認する。正しいものであることが確認できた場合には、内部状態記憶部207がμの内容に応じて、証明装置200の内部状態を変更する（S37）。変更後の内部状態の値をρに示す。入場の駅と時間が記録されたことがわかる。次に、内部状態記憶部207はこの内部状態の変更、すなわち入場記録の内容をM'とする。実施例1と同様に、証明情報生成部206は、M'の値を認証情報ρのビット列に連結して、チケット検証情報による署名を施した値Rを生成して、証明情報Rとして検証装置100に送る（S38）。

【0067】検証装置100は証明情報Rの値を検証し、その値が認証情報Cと一致した場合には、さらに内部状態を変更した結果M'を確認する。M'がμで指定したものと対応していれば、正しく内部状態が変更されたものと判断し、改札機のゲートを開ける。

【0068】次に、出場時の認証を説明する。出場時の認証は、入場時とは逆の経路であるが、相互に伝えられるメッセージの内容が異なる。

【0069】はじめに検証装置100は認証情報Cとともに、出場であることをあらわす情報を証明装置200に送る（S32）。

【0070】証明装置200のチケット判定情報生成部203はチケット判定情報Mを生成する。出場時のMの内容を図13に示す。証明情報生成部206は、MをCに連結し、チケット秘密鍵Dによる署名を施し、チケット証明情報Tとする。そして、証明情報Tと、認証情報生成部生成した第2の認証情報ρが検証装置100に送られる（S34）。

【0071】検証装置100の証明情報検証部104は、チケット証明情報を検証する。チケットの検証結果が正しい場合には、チケット判定部101が、チケット判定情報Mの内容を確認する。ここでは、入場駅が横浜駅で有効な入場記録であり、出場の有効期限内であることから、ここでの出場の認証が可能なチケットであると判定される（S35）。

【0072】次に、証明情報生成部103は証明装置200の内部状態を変更するための情報μを作成する。μ

(10)

特開平11-225143

17

の内容を図14に示す。 μ には、出場駅名と出場時間が記録される。証明情報生成部103は、さらに、生成された μ に結合し、検証装置の暗号情報 δ による署名を施した値 ρ を生成する。 ρ は証明装置200へと送られる(S36)。

【0073】証明装置200の証明情報検証部205は、送られた ρ の値が、認証情報 x と一致するかどうかを確認する。正しいことが確認できた場合には、内部状態制御部207が μ の内容に応じて、証明装置200の内部状態を変更し、この変更結果、すなわち出場記録を「M」とする。変更後の内部状態の様子を図15に示す。出場駅と時間が記録される。証明情報生成部206は、出場記録「M」を認証情報Cのビット列に連結して、チケット暗号情報による署名を施した証明情報Rを生成し、検証装置100に送る(S38)。

【0074】検証装置200の証明情報検証部104はRの値を検証し、その値が認証情報Cと一致した場合には、さらに内部状態を変更した結果「M」を確認する。「M」が μ の値で指定したものと対応していれば、正しく内部状態が変更されたものと判断し、出場を許可して、改札扉のゲートを開ける(S39)。

【0075】[実施例3]実施例3では、回数券のような形態を実現する方法を示す。

【0076】基本的に本実施例の構成やチケットの生成方法は、全体の処理の流れは実施例1と同様である。本実施例の全体の構成を図16に示す。本実施例の特徴として、内部状態の中に、回数券の残り度数を示すカウンタ202aが設置されている点が異なる。図16においては、図2と対応する箇所に対応する符号を付した。

【0077】利用者は回数券を購入すると、はじめに証明装置200に登録する。登録時に回数券に対応する内部状態記憶領域が確保され、そのなかのカウンタ202aに、残りの使用回数を書き込まれる。

【0078】回数券の利用時には利用者は、証明装置200に対してこれらを利用するチケットとして、チケット指定装置300により、回数券を指定した上で、検証装置100と証明装置200との間で認証プロトコルを開始される。

【0079】認証プロトコルでは、検証装置100が、認証情報として乱数Cを生成し証明装置200に送り、証明装置200が、チケット秘密鍵を計算するところまで、実施例1と同様である。

【0080】本実施例のチケット証明情報生成処理(図3のS33に対応)のフローチャートを図17に示す。図17において、証明装置200のチケット判定情報生成部203は、この回数券のチケットに対応した内部状態の残りの回数を抽出し、チケット利用情報とともに、チケット判定情報1に記録する(S81~S84)。そして、実施例1と同様に、証明情報生成部206がチケット証明情報Tを生成し(S85)、認証情報生成部20

18

4が第2の認証情報 x を生成する(S86)。Tと x は通信部208により検証装置100に送られる(S34)。

【0081】Tと x を受け取った検証装置100はチケット判定処理(図3のS35に対応)を行う。

【0082】チケット判定処理のフローチャートを図18に示す。図18において、検証装置100の証明情報検証部104は、受け取ったチケット証明情報を検証する(S91)。チケット証明情報が正しい場合には、チケット証明情報から、チケット判定情報Mを抽出する(S92)。チケット判定情報Mには回数券の残り回数

が記録されている。チケット判定部101はその値が1以上であれば、この回数券はまだ使用可能であると判断する(S93)。さらに、チケット利用情報1の内容も、この検証装置100で検証可能であるとチケット判定部101が判断した場合には、証明情報生成部103は証明装置200の内部状態の変更を示す情報 μ を作成する(S94、S95)。 μ の内容として、回数券の使用回数を1減らすことを指示する内容が含まれる。そして、実施例1と同様の方法で、 μ を使用して第2の証明情報 ρ を作成し(S96、S97)、証明装置200へと送る(S36)。

【0083】検証やチケット判定に失敗したときにはエラー処理を行う(S98)。

【0084】 ρ を受け取った証明装置200は内部状態変更処理(図3のS37に対応)を行う。

【0085】内部状態変更処理のフローチャートを図19に示す。図19において、証明装置200の証明情報検証部205は送られた第2の証明情報 ρ を検証する(S101)。正しいものであることが確認できた場合には、内部状態制御部207が μ の内容に応じて、回数券の残り使用回数を1減らし、その結果を「M」とする(S102~S104)。あとは、実施例1と同様の方法で、証明装置200の認証情報Rを生成して、検証装置100に送る(S105、S106)。ステップS101で検証に失敗したときにはエラー処理が行われる(S107)。

【0086】以降の検証装置100の動作は、実施例1と同様であり、Rの値を検証して、サービスの提供を行う。

【0087】[実施例4]本発明の実施例4では、全体の構成は実施例1と同様であるが、チケット公開情報・チケット秘密情報やチケットの認証方法が異なる。

【0088】本実施例では、 g が素数であり、 G が有限群 G の位数 ϕ の元であり、

$$[数14] y = g^x \bmod p$$

が満たされるとき、 (p, G, g, y) がチケット公開情報であり、 x をチケット秘密情報とする。 $(p, G,$

19

g) はシステム全体で共通とすることもできる。

【0090】このとき、チケットはチケット特長情報xと証明装置固有情報duとチケット利用情報しと、群を規定する情報pより、

【0091】

【数15】 $t = x - F\{du, L, y, p\}$

として、計算される。ここで、Fは非直交性の一方関数であり、一般のハッシュ関数によって実用可能である。しは実施例1と同様のチケット利用情報である。

【0092】また、検証装置の特長をあらわすものとし、

【0093】

【数16】

$$n = g^f \bmod p$$

を満たすような力を公開情報、を秘密情報とする。

【0094】実際にはGを乗法群として構成したり、有限体上の楕円曲線として構成することができる。

【0095】本発明の認証プロトコルの概略を図20に示す。

(11)

待時間11-225143

20

* 【0096】はじめに利用者は、これから利用するチケットを証明装置に対して指定した上で、検証装置と証明装置の間で認証プロトコルを開始される。

【0097】図20において、この認証プロトコルでは、まず検証装置100の認証情報生成部102が、乱数rを生成し、 $C = g^r$ を計算して、これを認証情報として証明装置に送る(S201、S202、S203)。

【0098】認証情報Cを受け取った証明装置200は、チケット証明情報生成処理を実行する(S204)。

【0099】チケット証明情報生成処理のフローチャートを図21に示す。図21において、まず証明装置200の証明情報生成部206は、署名に用いる秘密鍵xを、チケットとチケット利用情報し、チケット公開情報のp、および証明装置固有情報duから、以下の計算により算出する(S211)。

【0100】

【数17】

$$t = F\{y, L, du, p\}$$

$$= x - F\{y, L, du, p\} + F\{y, L, du, p\}$$

$$= x$$

次に、チケット判定情報生成部203は、正しいチケットを保持していることを示すためのチケット判定情報Mを、チケットの付加情報しと内部状態の情報から生成する(S212)、証明情報生成部206は、証明情報として、以下の値を生成する(S213、S214)。

【0101】

【数18】 $T = \{C || M\} \cdot C^r \bmod p$

なお証明情報Tは上記以外にも、以下の式によっても計算できる。

【0102】

【数19】

$$T = \{C || M\} \cdot C^r \cdot C^{(y, L, du, p)} \bmod p$$

また、認証情報生成部204は同時に乱数r'を生成して、

【0103】

$$\text{【数20】 } x = g^{r'} \bmod p$$

を第2の認証情報として検証装置に送る(S215、S216、S205)。チケット判定情報Mに入る情報は実施例1〜3と同様である。

【0104】証明情報Tと第2の認証情報xは、通信部208により検証装置100に送られる。

【0105】Tとxを受け取った検証装置100はチケット判定処理(図20のS206)を行う。

【0106】チケット判定処理のフローチャートを図22に示す。図22において、検証装置100の証明情報検証部103は、送られたチケット証明情報から、

【0107】

$$\text{【数21】 } T/y^r \bmod p = \{C || M\} \cdot C^r / 50$$

$y^r \bmod p$ の値を計算し、そのビット列のうち、連結されたM以外の部分が、認証情報Cと一致するかどうかを確認する(S221)。

一致した場合には、チケット判定部101はさらにチケット判定情報Mの内容から、チケット及びチケットに関連付けられた内部状態がこの検証装置100で検証して良いものかどうかを判定する(S222、S223)。判定の結果、このチケットを検証して良い場合には、証明情報生成部103は検証装置200の内部状態の変更を指示する情報μを作成して、xに連結する(S224、S225)。そして、この値に対して、検証装置の特長を表す秘密情報を用いて以下の値を第2の認証情報として、生成する(S226)。

【0108】

【数22】

$$\rho = (x || \mu) \cdot x^r \bmod p$$

ρは通信部108により証明装置200へと送られる。一方、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないもの場合には、プロトコルを終了する(S227)。

【0109】次にρを受け取った証明装置200は内部状態変更処理(図20のS208)を行う。

【0110】内部状態変更処理のフローチャートを図23に示す。図23において、証明装置200の証明情報検証部205は、送られた応答情報から、

【0111】

【数23】

(32)

特開平 11-225143

$$\rho/\eta^r \bmod p = \{x \mid \mu\} \cdot x^r/\eta^r \bmod p$$

の値を計算し、そのビット列のうち、過剰された μ 以外の部分が、第2の検証結果と一致するかどうかを確認する(S231)。正しいものであることが確認できた場合には、内部状態制御部207が、 μ の内部状態の変更を指示する情報に応じて、証明結果200の内部状態が変更し、その結果をM'とする(S232~S234)。一方、確認の結果、正しくないことが判明した場合には場合には、プロトコルを終了する(S137)。

【0112】証明情報生成部206は、M'の値を証明情報Cのビット列に連結した上で、以下の値を証明情報として生成する(S235、S236)。

【0113】

【数24】 $R = \{C \parallel M'\} \cdot C^* \bmod p$
 こうして生成された証明情報Rが通信部208により検証装置100に送られる(S209)。

【0114】Rを受け取った検証装置100は、証明情報検証処理部210(図20)を行う。

【0115】証明情報検証処理部のフローチャートを図24に示す。図24において、証明情報検証部104は、送られたチケット証明情報から、

【0116】

【数25】 $R/\eta^r \bmod p = \{C \parallel M'\} \cdot C^* / \eta^r \bmod p$

の値を計算し、その結果M'を除いた上位のビット列が、最初に検証装置100が生成した認証情報Cと一致することを確認する(S241)。確認できた場合は、さらに内部状態の変更結果を表す情報M'の内容が、第2の証明情報として送った、内部状態変更を許可する情報 μ と一致するかどうかを確認し(S242、S243、S244)。確認ができた場合には、定められたサービスを提供することができ、利用者の意図しない内部状態の変更や、内部状態の変更による不正行為を防止することができる。

【0117】

【発明の効果】以上で説明したように、本発明によれば、検証装置が検証可能なチケットのみを検証し、検証することが正しくないチケットに対しては、内部状態の変更を許可する情報を生成しないような電子チケットシステムを実現することができ、利用者の意図しない内部状態の変更や、内部状態の変更による不正行為を防止することができる。

【図面の簡単な説明】

【図1】 関連技術の処理を説明するフローチャートである。

【図2】 実施例1、2、4の構成を全体として示すブロック図である。

【図3】 実施例1の処理全体を説明するフローチャートである。

【図4】 実施例1の証明装置のチケット証明情報生成

処理を説明するフローチャートである。

【図5】 実施例1の検証装置のチケット判定処理を説明するフローチャートである。

【図6】 実施例1の証明装置の内部状態変更処理を説明するフローチャートである。

【図7】 実施例1の検証装置の証明情報検証処理を説明するフローチャートである。

【図8】 実施例2のトークンの初期の内部状態を示す図である。

【図9】 チケット付加情報の項目を示す図である。

【図10】 入場時にトークンから改札機に送られるチケット判定情報Mを示す図である。

【図11】 入場時に改札機からトークンに送られる項目 μ を示す図である。

【図12】 入場後のトークンの内部状態を示す図である。

【図13】 出場時にトークンから改札機に送られるチケット判定情報Mを示す図である。

【図14】 出場時に改札機からトークンに送られる情報 μ を示す図である。

【図15】 出場後のトークンの内部状態を示す図である。

【図16】 実施例3の構成を全体として示すブロック図である。

【図17】 実施例3の証明装置のチケット証明情報生成処理を説明するフローチャートである。

【図18】 実施例3の検証装置のチケット判定処理を説明するフローチャートである。

【図19】 実施例3の証明装置の内部状態変更処理を説明するフローチャートである。

【図20】 実施例4の処理を全体として示すフローチャートである。

【図21】 実施例4の証明装置のチケット証明情報生成処理を説明するフローチャートである。

【図22】 実施例4の検証装置のチケット判定処理を説明するフローチャートである。

【図23】 実施例4の証明装置の内部状態更新処理を説明するフローチャートである。

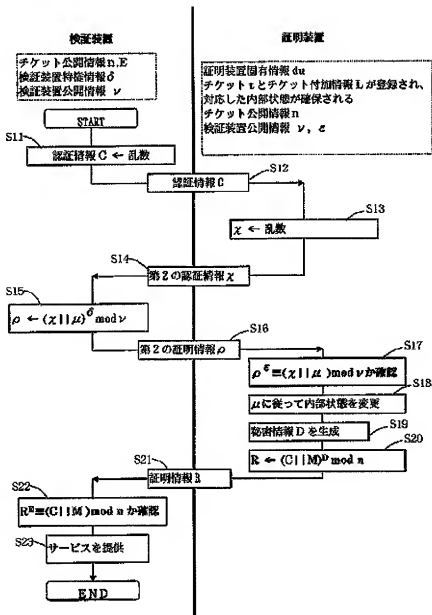
【図24】 実施例4の検証装置の証明情報検証処理を説明するフローチャートである。

【符号の説明】

100 検証装置
 101 チケット判定部
 102 認証情報生成部
 103 証明情報生成部
 104 証明情報検証部
 200 証明装置
 201 証明装置固有情報保持部
 202 チケット保持部

		(13)	特開平11-225143
202a	カウンタ	23	24
203	チケット判定情報生成部	*206	証明情報生成部
204	認証情報生成部	207	内部状態制御部
205	証明情報検査部	300	チケット指定装置
		*	

【図1】

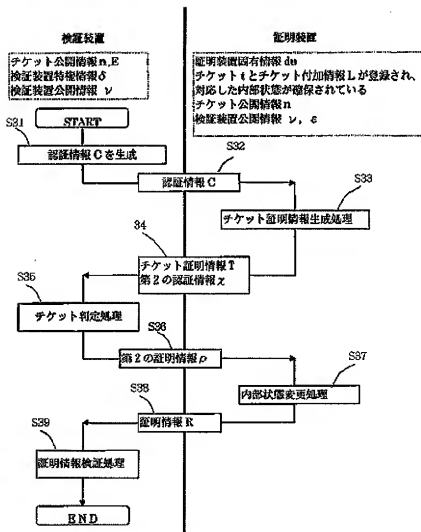


関連技術の処理のフローチャート

(15)

特開平 11-225143

【圖 3】



実施例1の処理全体のフローチャート

【圖 11】

入場券	入場時間
席番	2017/10/01

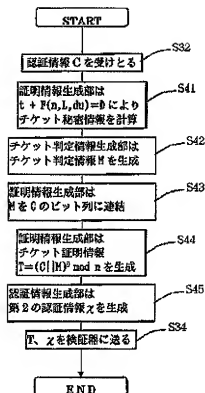
【圖 12】

チケット	発行年度	発行枚数	発行期間	入場回数	出場記録	残高
0001	07/01/01	発売	なし	なし	なし	なし
0008	07/01/01	チケット	なし	07/01/01, 07/01/02	07/01/01, 07/01/02	なし
0005	07/01/01	チケット	なし	07/01/01, 07/01/02	07/01/01, 07/01/02	なし

(16)

特開平 1 1 - 2 2 5 1 4 3

【図 4】



実施例 1 の証明装置のチケット証明情報生成処理のフローチャート

【図 1 3】

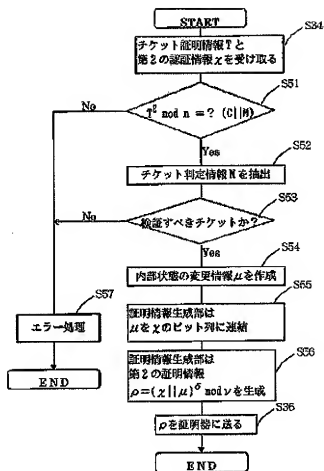
出発駅にトークンから改札機に送られるチケット判定情報 M

出発駅	目的地	使用開始日	有効 期間	経路	入場記録	出場 記録	改札 記録
横浜	成田空港	97/7/18	1 日	東京	97/7/18, 8:20 横浜	なし	なし

(17)

特開平11-226143

【図5】



実施例1の検証装置のチケット判定処理のフローチャート

【図14】

証明情報	証明情報
証明情報	07/25, 8, 23

出願時に改訂されたトークンに送られる情報、μ(証明情報で証明)

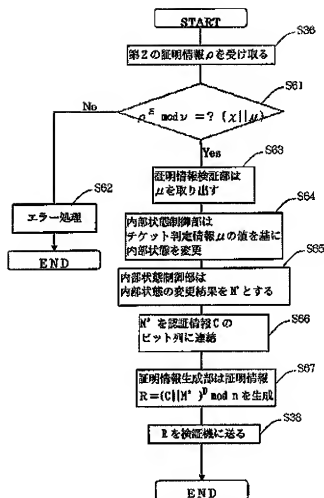
【図15】

出願時のトークンの内容に関する					
チケットID	発行時刻	発行場所	発行時刻	発行時刻	発行時刻
0001	07/25	東京	なし	なし	なし
0002	07/25	千葉	なし	07/25, 8, 23	07/25, 8, 23
0003	07/25	東京	なし	07/25, 8, 23	07/25, 8, 23

(18)

特開平11-225143

【図6】

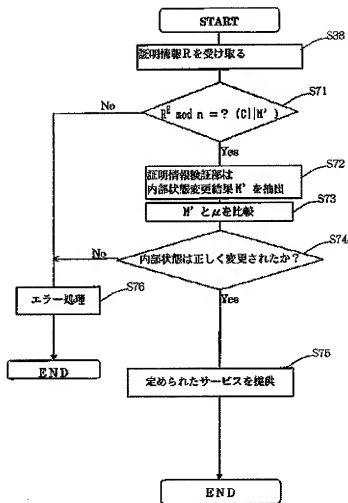


実施例1の証明装置の内部状態更新処理のフローチャート

(19)

特開平 11-225143

【図 7】

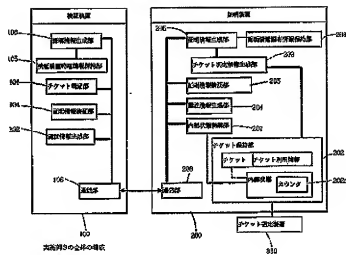


実施例 1 の検証装置の証明情報検証処理のフローチャート

(20)

特開平11-225143

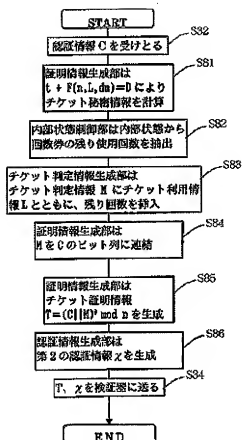
【圖 16】



(21)

特開平11-225143

【図17】

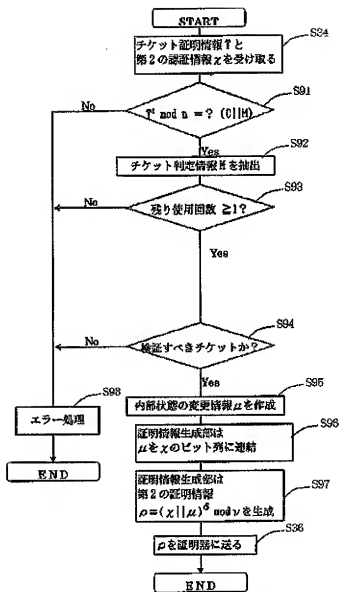


実施例3の証明装置のチケット証明情報生成処理のフローチャート

(22)

特開平11-225143

【図18】

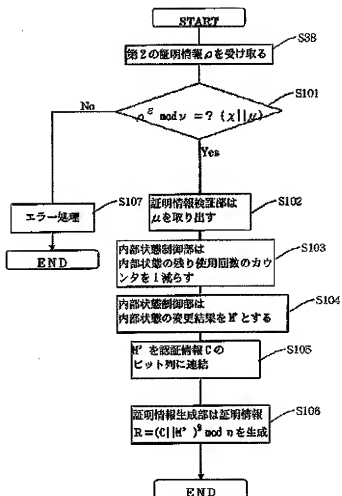


実施例3の検証装置のチケット判定処理のフローチャート

(23)

特開平11-225143

【図19】

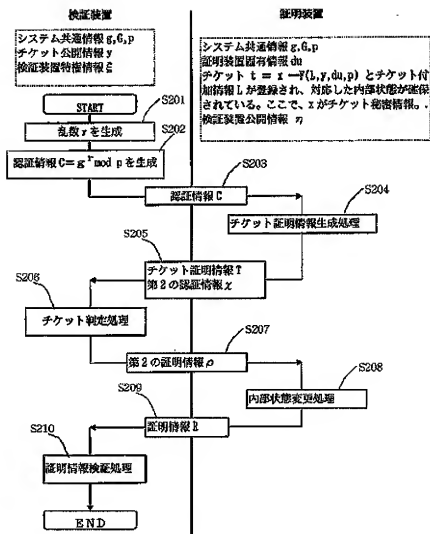


実施例3の証明装置の内部状態変更処理のフローチャート

(24)

特開平11-225143

【図26】

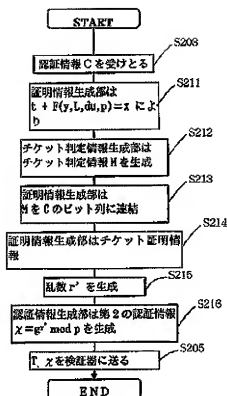


実施例4の処理全体のフローチャート

(25)

特開平11-225143

【図21】

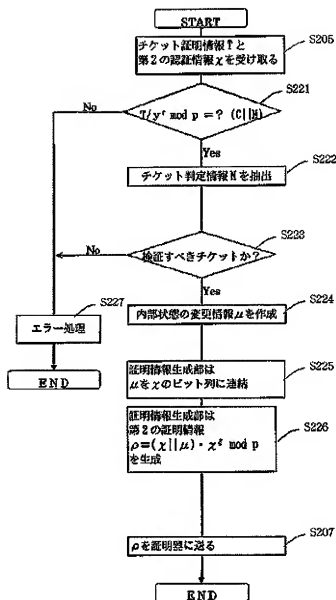


実施例 4 の証明情報のチケット証明情報生成処理のフローチャート

(26)

特開平11-225143

【図22】

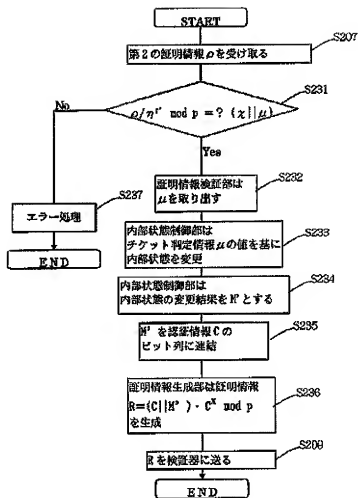


実施例4の検証装置のチケット判定処理のフローチャート

(27)

特開平11-225143

【図23】

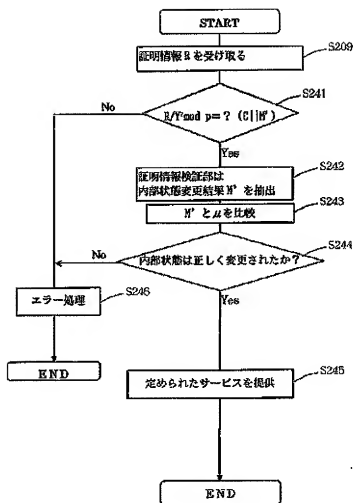


実施例4の証明装置の内部状態更新処理のフローチャート

(28)

特開平 11-225143

【図 24】

実施例 4 の検証装置の証明情報検証処理のプロローチャート

フロントページの続き

(51) Int. Cl.⁹
 G 0 7 B 1/00
 5/00
 G 0 7 F 7/12
 G 0 9 C 1/00

識別記号
 6 6 0

F I
 G 0 7 B 5/00 C
 G 0 9 C 1/00 6 6 0 Z
 G 0 6 F 15/21 3 4 0 C
 G 0 7 F 7/08 C
 H 0 4 L 9/00 6 7 6 Z

(29)

特開平11-225143

(72)発明者 谷口 誠一郎
神奈川県足柄上郡中井町境430 グリーン
テクナかし、高士ゼロックス株式会社内